Case C-77/21

Request for a preliminary ruling

Date lodged:

8 February 2021

Referring court:

Fővárosi Törvényszék (Hungary)

Date of the decision to refer:

21 January 2021

Applicant:

Digi Távközlési és Szolgáltató Kft.

Defendant:

Nemzeti Adatvédelmi és Információszabadság Hatóság

Fővárosi Törvényszék (Budapest High Court, Hungary)

[…]

Applicant: Digi Távközlési és Szolgáltató Kft. ([…] Budapest, Hungary)

[…]

Defendant: Nemzeti Adatvédelmi és Információszabadság Hatóság (National Authority for Data Protection and Freedom of Information) ([…] Budapest, Hungary)

[…]

Subject matter of the dispute: Administrative-law action concerning data protection […]

Order

This court […] refers the following questions to the Court of Justice of the European Union for a preliminary ruling:

1. Must the concept of ‘purpose limitation’ as defined in Article 5(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 (the 'Regulation'), be interpreted as meaning that the fact that the controller stores in parallel in another database personal data which were otherwise collected and stored for a limited legitimate purpose is consistent with that concept or, conversely, is the limited legitimate purpose of collecting those data no longer valid so far as the parallel database is concerned?

2. Should the answer to the first question referred be that the parallel storage of data is in itself incompatible with the principle of 'purpose limitation', is the fact that the controller stores in parallel in another database personal data which were otherwise collected and stored for a limited legitimate purpose compatible with the principle of 'storage limitation' established in Article 5(1)(e) of the Regulation?

[…] [matters of domestic procedural law]

Grounds

Facts

1 The applicant is one of the leading internet and television providers in Hungary.

2 In April 2018, with a view to conducting tests and correcting errors, the applicant created a database known as the 'test' database (the 'test database') to which it copied the personal data of approximately one third of its private customers. In another database known as the 'digihu' database, linkable to the digi.hu website, it stored, for direct marketing purposes, the up-to-date data of newsletter **[Or. 2]** subscribers and of systems administrators that provide access to the website interface. This database contained the data of almost 3% of its private customers and the user data of forty systems administrators with full or partial administration rights.

3 On 23 September 2019, the applicant became aware that the personal data (name, mother's name, place and date of birth, address, identity card number or, as the case may be, personal number, e-mail address, landline and mobile telephone numbers) of a total of some 322 000 data subjects (297 000 customers and subscribers and 25 000 newsletter subscribers) had been accessed via the www.digi.hu website. It was the hacker himself who alerted the applicant to the attack, in writing, in an e-mail of 21 September 2019, in the process producing, by way of evidence, one of the records from the database and explaining the technicalities of the error. The applicant then corrected the error, concluded a confidentiality agreement with the ethical hacker and offered him a reward. The 'digihu' database was not affected by the attack but it could have been.

4 On 25 September 2019, the applicant reported the personal data security breach to the defendant, which responded by launching an official review procedure on 8 October 2019.

5 By decision […] of 18 May 2020, the defendant found as follows:

(a) that the applicant had infringed Article 5(1)(b) and (e) of the Regulation in having neglected, once the necessary tests and corrections of errors had been carried out, to delete the test database affected by the data security breach, which was originally created to correct errors, and in having thereby stored in the test database a large volume of customer data for almost a further year and a half for no purpose and in such a way as to allow those customers to be identified, and that the failure to take the measure (to delete the test database) had directly facilitated the personal data security breach;

(b) that the applicant had infringed Article 32(1) and (2) of the Regulation.

The defendant ordered the applicant to review all its databases containing personal data with a view to determining whether there were grounds for applying an encryption system to them and to inform it of the outcome of that review. It also imposed on the applicant a data protection fine in the amount of HUF 100 000 000 and ordered that the decision be published.

6 In the grounds of its decision, the defendant cited the following provisions of the Regulation: Article 2(1); Article 4(12); Article 5(1)(b) and (e) and (2); Article 17(1)(a); Article 32(1)(a) and (2); and Article 33(1), (2), (4) and (5).

7 The defendant noted that the Regulation has been applicable in Hungary since 25 May 2018 and that, since the data processing affected by the personal data security breach (storage of customer data) carried on after that date, the Regulation was applicable in this case pursuant to Articles 2(1) and 99(2).

8 It stated that the purpose of creating the test database (to conduct tests and correct errors) was different from the initial purpose of processing the personal data stored in the database (to perform contracts), given that correcting the errors had also caused the purpose other than data processing (to conduct tests and correct errors) to disappear. Consequently, the failure to delete the databases after the errors had been corrected constituted an infringement of the fundamental principle of ‘storage limitation’.

9 As regards data security measures relating to data storage, the defendant took the view, principally, that the data security breach could be put down to the – long-known about and repairable – vulnerability of the ‘Drupal’ content management system used by the applicant, the errors in which the applicant had not corrected because the available repair package was not official. Relying on an expert report on information security which had been submitted in the course of the procedure, the defendant stated that the security breach could have been remedied with appropriate software, regular vulnerability checks and appropriate encryption, but

the applicant, in not taking such measures, had infringed Article 32(1) and (2) of the Regulation.

10 In addition, the defendant imposed on the applicant a data protection fine in accordance with Article 83(2) of the Regulation and certain provisions of the az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Law CXII of 2011 on the right to self-determination as regards information and freedom of information).

Subject matter of the dispute

11 The applicant brought an administrative-law action against the defendant's decision. **[Or. 3]**

12 As regards the principle of 'purpose limitation', the applicant claims that the customer data transferred to the databases in question were collected legitimately for the purposes of concluding subscription contracts, in accordance with Article 6(1)(b) of the Regulation, and that that purpose did not change when the test database affected by the data security breach was created. The applicant created the test database in order to store the data in question so as to continue to have them available for the legitimate purpose for which they were initially collected. Consequently, the creation of the test database, that is to say, the act of storing the data collected in another internal system, is not incompatible with the purpose of collecting those data. The applicant submits that the principle of 'purpose limitation' does not indicate in which internal system the controller may process legitimately collected data, any more than it prohibits the copying of legitimately collected data. The applicant claims that the scope of the personal data processed was not extended by the creation of the test database and that, in so far as the creation or retention of that database may have increased the risks to the security of the data, this cannot be considered to be an infringement of a basic principle, but may, at most, be regarded as a data security issue for the purposes of Article 32 of the Regulation. It therefore claims that, in also keeping in the test database customer data stored for a legitimate purpose, it did not infringe Article 5(1)(b) of the Regulation.

13 As regards the principle of 'storage limitation', the applicant claims that, since the customer data were not processed with a view to correcting errors, the data storage period cannot be determined by the purpose of correcting errors. Consequently, it did not fail to fulfil the data storage requirement by not deleting the test database immediately after the errors had been corrected, since it was entitled to store the data contained in the test database in such a way as to allow the data subjects to be identified, irrespective of any correction of errors. Nor, therefore, can it be accused of infringing Article 5(1)(e) of the Regulation.

14 The applicant has asked the referring court to submit to the Court of Justice of the European Union a request for a preliminary ruling on, inter alia, the foregoing matters.

15 The defendant contends that the applicant's claims should be dismissed. It submits that, in this instance, there is no relevant question capable of forming the subject of a preliminary ruling.

Relevant EU law

16 According to Article 5(1)(b) of the Regulation, on principles relating to the processing of personal data, such data are to be 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 is, in accordance with Article 89(1), not to be considered incompatible with the initial purposes ('purpose limitation').

17 In accordance with Article 5(1)(e) of the Regulation, personal data are to be 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').

Relevant Hungarian law

18 The Regulation is in force in Hungary and has been applicable since 25 May 2018. The questions referred for a preliminary ruling relate to the application of the Regulation. **[Or. 4]**

Reasons why the request for a preliminary ruling is necessary

19 The matters on which the referring court seeks guidance from the Court of Justice of the European Union concern the interpretation to be given to the principle of purpose limitation established in Article 5(1)(b) of the Regulation and to the principle of storage limitation established in Article 5(1)(e) of the Regulation.

20 The customer data which the applicant incorporated into the test database affected by the data security breach were collected for the purposes of concluding subscription contracts, in accordance with Article 6(1)(b) of the Regulation, and the lawfulness of this has not been called into question by the defendant.

21 The referring court asks whether the copying to another database of data which, as is common ground between the parties, were collected for a limited purpose changes the purpose of collecting and processing the data. It also falls to be

determined whether the fact of creating a test database (that is to say, keeping in another system data collected for a limited purpose) and continuing to process those customer data in this way is compatible with the purpose of collecting the data.

22 The referring court takes the view that the principle of purpose limitation does not provide any clear indication as to which of the controller's internal systems are ones in which the controller may process legitimately collected data, or whether that controller may copy such data to a test database without changing the purpose of collecting the data.

23 If creating a test database (that is to say, keeping data in another internal system) is not compatible with the purpose of collecting the data, the referring court asks, in connection with the principle of storage limitation, whether, in so far as the purpose of processing the customer data in another database was not to correct errors but to conclude contracts, the necessary storage time is determined by the correction of errors or by the performance of contractual obligations.

24 […] [matters of domestic procedural law]

25 […] [matters of domestic procedural law]

Final part

Budapest, 21 January 2021.

[…] [Signatures]