Reports of Cases

OPINION OF ADVOCATE GENERAL
ĆAPETA
delivered on 6 October 2022 [1]

Case C-268/21

Norra Stockholm Bygg AB
v
Per Nycander AB,
joined parties:
Entral AB

(Request for a preliminary ruling from the Högsta domstolen (Supreme Court, Sweden))

(Reference for a preliminary ruling – Regulation (EU) 2016/679 – Protection of personal data – Article 6(3) and (4) – Processing of personal data – Article 23(1)(f) – Protection of judicial independence and judicial proceedings – Request of the respondent in civil proceedings to order the appellant to produce information on the hours worked by its employees)

I. Introduction

1. 'Your privacy is important for us. We use cookies to improve the user experience. Please review privacy preferences. Accept all / Settings. Check our privacy policy and cookies policy'. [2]

2. Upon visiting any website, a message of a similar kind will pop up.

3. That is the result of the General Data Protection Regulation ('the GDPR'), [3] which has become the main instrument for the protection of personal data in the European Union.

4. Does the GDPR also pop up before national courts? More specifically, does it apply to disclosure obligations in a civil procedure before a national court? If it does, what obligations does it create for those courts? These are the issues that the Court is invited to clarify in this case.

1 Original language: English.

2 This particular message appears at https://eulawlive.com/.

3 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).

II. The facts in the main proceedings and the questions referred for a preliminary ruling

5. Those issues arose in a case before the referring court, the Högsta domstolen (Supreme Court, Sweden). The facts of the case can be summarised as follows. Norra Stockholm Bygg AB ('Fastec'), the appellant in the main proceedings, carried out the construction of an office building for Per Nycander AB ('Nycander'), the respondent in the main proceedings. The employees carrying out the work under that contract recorded their presence in an electronic staff register for tax purposes. The staff register was provided by Entral AB, acting on behalf of Fastec.

6. The main proceedings began with a dispute concerning the compensation due for the work carried out. Nycander has challenged Fastec's payment request (amounting to just over 2 000 000 Swedish kronor (SEK), approximately 190 133 EUR), claiming that the amount of time that Fastec spent on the work was less than the period in respect of which Fastec is claiming payment.

7. To prove that this is the case, Nycander requested that Entral produce the staff register it kept on behalf of Fastec. Fastec is opposing that request, claiming that such a disclosure would breach the GDPR, as the requested data were collected for another purpose and cannot be used as evidence in the main proceedings.

8. The Tingsrätt (District Court, Sweden) ordered Entral to produce the register, and this decision was upheld on appeal by the Svea hovrätt (Svea Court of Appeal, Stockholm, Sweden).

9. Fastec appealed against the decision of the Svea hovrätt (Svea Court of Appeal, Stockholm) before of the Högsta domstolen (Supreme Court), and asked that court to reject Nycander's request for disclosure or, in the alternative, to order that an anonymised version of the staff register be produced. It is in the context of that procedure that the Högsta domstolen (Supreme Court) submitted a request for a preliminary ruling to the Court of Justice with the following questions:

'(1) Does Article 6(3) and (4) of the [GDPR] also impose a requirement on national procedural legislation relating to disclosure obligations?

(2) If Question 1 is answered in the affirmative, does the [GDPR] mean that regard must also be had to the interests of the data subjects when a decision on disclosure must be made which involves the processing of personal data? In such circumstances, does EU law establish any requirements concerning how, in detail, that decision should be made?'

10. In the course of the proceedings, written observations were submitted to the Court by Fastec, the Czech, Polish, and Swedish Governments and the European Commission. A hearing was held on 27 June 2022 where Nycander, the Polish and Swedish Governments, and the Commission presented oral argument.

III. Legal framework

A. European Union law

11. Article 5 of the GDPR determines the principles that any processing of personal data must comply with:

'1. Personal data shall be:

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

(b) 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");

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

(d) 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");

(e) 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");

(f) 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").'

12. Article 6 of the GDPR, entitled 'Lawfulness of processing', in its paragraphs 1, 3 and 4 provide as follows:

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

…

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

…

(e) 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;

…

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.'

13. Furthermore, Article 23(1) of the GDPR regulates restrictions of rights and obligations under the GDPR:

'1. Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard:

…

(f) the protection of judicial independence and judicial proceedings;

…'

B. Swedish law

14. The first subparagraph of Paragraph 2 of Chapter 38, of the rättegångsbalken (Code of Judicial Procedure; 'the RB') provides that any person in possession of a written document which may be deemed to have probative value is required to produce that document. The second subparagraph of the same provision sets out exceptions to such an obligation, including lawyers, doctors, psychologists, priests and other officials who have been entrusted with information while carrying out their profession or equivalent. Paragraph 4 of Chapter 38 of the RB then grants a court the power to order the disclosure of a written document as evidence.

15. According to the referring court, when considering whether a person should be obliged to produce a document, a court must weigh up the relevance of the evidence against the opposing party's interest in not releasing that information. However, as the referring court explains, this does not involve taking into account the private nature of the information being disclosed.

IV. Analysis

A. Setting the stage

16. The GDPR is the main EU act regulating the protection of natural persons regarding the processing of their personal data. Unlike its predecessor, Directive 95/46/EC,[4] the GDPR was adopted on the basis of Article 16 TFEU.[5] That legal basis empowered the EU legislature to safeguard the fundamental right to protection of personal data, provided for in Article 8(1) of the Charter of Fundamental Rights of the European Union ('the Charter').[6]

17. When personal data are processed, the GDPR places the responsibility for compliance with that act on the 'data controller'.[7] In every instance of personal data processing, it is, therefore, important to establish who the data controller is.

18. In accordance with Article 4(7) of the GDPR, the data controller is the natural or legal person, public authority, agency or other body, which determines the purposes and means of the processing of personal data.

19. In the case at hand, two separate instances of processing of personal data took place. The first processing concerns the electronic staff register maintained by Entral on behalf of Fastec, the latter being under an obligation, envisaged by Swedish law, to collect data on hours worked for tax purposes. In this context, Fastec is the controller and Entral is the processor.[8]

20. It is not disputed that this first processing was in compliance with the GDPR. Specifically, Article 6(1)(c) thereof allows processing of personal data necessary for compliance with a legal obligation to which the controller, in this case Fastec, is subject.[9] Certainly, if this first processing were to be found unlawful under the GDPR, the repurposed processing of such data would, by extension, be unlawful as well.[10]

4 Directive 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). Directive 95/46 was adopted on the internal market legal basis. For an initial analysis of the changes introduced by the GDPR, see Van Alsenoy, B., 'Liability under EU Data Protection Law. From Directive 95/46 to the General Data Protection Regulation', *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, Vol. 7, 2016, 271-288.

5 Despite their difference in legal basis, the case-law interpreting Directive 95/46 is relevant for understanding the GDPR. See, in that respect, judgment of 17 June 2021, *M.I.C.M.* (C-597/19, EU:C:2021:492, paragraph 107). I will therefore refer to the Court's case-law concerning Directive 95/46 where relevant. Likewise, to the extent that it provides analogous solutions to restrictions to the right to data protection, I will also refer to the Court's case-law concerning Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37). The Court considered that the interpretation of restrictions to the rights stemming from Directive 2002/58 are to apply, *mutatis mutandis*, to the interpretation of the GDPR. See in that respect the judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791, paragraphs 209 to 211).

6 See recital 1 of the GDPR.

7 See Article 5(2) of the GDPR.

8 Article 4(8) of the GDPR defines the processor as: 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'.

9 According to Article 6(3) of the GDPR, when processing is carried out for the purpose of compliance with a legal obligation to which the data controller is subject, such basis shall be laid down by European Union or Member State law that meets the objective of public interest and is proportionate to the legitimate aim pursued. Compliance with national tax legislation was deemed a legitimate purpose in the judgment of 16 January 2019, *Deutsche Post* (C-496/17, EU:C:2019:26, paragraphs 60 to 63).

10 See, by analogy, judgment of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152, paragraph 44).

21. The interest of this case is, however, the second (repurposed) processing of the same data that was originally collected for tax purposes. The new purpose is the disclosure, by Entral, of the staff register as evidence in the civil proceedings between Fastec and Nycander. Producing that register for its use in civil proceedings would necessarily entail processing of personal data.

22. In that second processing, the roles under the GDPR change in comparison to the first processing. Most importantly, by issuing the order to Entral to produce the staff register ('the order for disclosure'), the national court is the entity determining the purposes and means of the second data processing.[11] That court, therefore, becomes the data controller.[12]

23. In that second processing, Fastec might be seen as remaining the controller, or having changed role: now being the recipient of data, together with Nycander.[13] However, even if Fastec remains the controller jointly with the national court,[14] that would not influence the obligations of the national court as controller.[15] Finally, the role of Entral does not change. It remains the processor and continues to process the same personal data, but now on behalf of the new controller, the national court.

24. By its first question, the referring court asks essentially whether the national court can indeed become a controller under the GDPR, and whether, in that case, that regulation imposes requirements on national procedural legislation relating to the powers and obligations of courts in civil proceedings. If the GDPR applies and the national court is the controller, the referring court asks, in its second question, how such a court should decide on the disclosure of personal data when they are to be used as evidence in civil proceedings.

25. To answer the questions of the referring court, I will proceed as follows. I will first explain why I consider the GDPR applicable to civil proceedings before Member States' courts and how that influences the Member States' existing procedural legislation (B). Thereafter, I will deal with the methodology which national courts as data controllers should apply to satisfy the requirements of the GDPR (C).

[11] Determining the purpose and means of processing of personal data are the central activities that determine who is the controller. See judgment of 10 July 2018, *Jehovan todistajat* (C-25/17, EU:C:2018:551, paragraph 68). See also Bygrave, L.A. and Tossoni, L., 'Article 4(7). Controller' in Kuner, C., Bygrave, L.A., Docksey, C. and Drechsler, L. (eds), *The EU General Data Protection Regulation (GDPR): A Commentary*, OUP, Oxford, 2021, at p. 150.

[12] At the hearing, the Polish and Swedish Governments and the Commission agreed that this role now pertains to the national court. Nycander maintained that Fastec remains the sole data controller in the second processing, while the role of the national court is that of an intermediary. It should be noted that the term 'intermediary' is not used anywhere in the GDPR.

[13] Article 4(9) of the GDPR defines recipients as natural or legal persons, public authorities, agencies of other bodies to which the personal data are disclosed, whether they are a third party or not. As parties in a civil procedure, both Fastec and Nycander will become recipients of data processed on the basis of the court's disclosure order. The Commission at the hearing maintained that Fastec remains the controller, rather than it having become the recipient.

[14] Article 26(1) of the GDPR provides: '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.' See also judgment of 29 July 2019, *Fashion ID* (C-40/17, EU:C:2019:629, paragraph 67).

[15] The Court explained that the concept of a controller is a broad one and different operators may be involved at different stages of the processing. Judgment of 29 July 2019, *Fashion ID* (C-40/17, EU:C:2019:629, paragraph 70).

B. The GDPR is applicable to civil proceedings before national courts and complements Member States' procedural rules

26. The first question of the referring court asks essentially whether the GDPR applies to civil judicial proceedings and what influence it has on the pertinent procedural rules. More specifically, it questions whether it affects those national rules that govern the powers and obligations of courts in ordering the disclosure of documentary evidence. I will answer this question in three steps.

1. The GDPR does not exclude the activities of national courts in civil proceedings

27. The material scope of the GDPR is defined in Article 2(1) thereof and takes a functional, rather than an institutional approach. It is the *what* (the activity of processing of personal data) rather than the *who*, that triggers the applicability of the GDPR. [16]

28. Situations excluded from the scope of the GDPR, enumerated in Article 2(2) thereof, are likewise functional in nature. Given that they represent the exception to the application of the GDPR, the Court considered that they should be interpreted restrictively. [17]

29. The activities of public authorities are therefore not excluded from the scope of the GDPR as such, but rather solely in relation to the activities enumerated in Article 2(2) of the GDPR. [18] In that respect, that provision does not exclude judicial activities in civil procedures from the material scope of the GDPR.

30. The conclusion that the GDPR applies to judicial activities is corroborated by recital 20 of the GDPR, [19] which states that that act applies to the activities of courts and other judicial authorities. [20]

31. The exclusion of the competence of supervisory authorities over courts when they act in their judicial capacity, set out in Article 55(3) of the GDPR, does not affect the previous conclusion. Quite to the contrary, to my mind, that provision confirms that courts acting in their judicial capacity are subject to the obligations imposed by the GDPR. It safeguards their independence and impartiality by prohibiting oversight by a supervisory body of their processing operations.

16 The latter is only exceptionally relevant. For example, under Article 2(3) of the GDPR, EU institutions, bodies, offices and agencies are not subject to the GDPR. Nevertheless, they are subject to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001 L 8, p. 1).

17 Judgment of 9 July 2020, *Land Hessen* (C-272/19, EU:C:2020:535, paragraph 68).

18 Article 2(2) of the GDPR provides: 'This Regulation does not apply to the processing of personal data: (a) in the course of an activity which falls outside the scope of Union law; (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU; (c) by a natural person in the course of a purely personal or household activity; (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'

19 Recital 20 of the GDPR states as follows: 'While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. It should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.'

20 See, in that respect, judgment of 24 March 2022, *Autoriteit Persoonsgegevens* (C-245/20, EU:C:2022:216, paragraphs 25 and 26).

32. The present case involves the processing of personal data, which falls within the material scope of the GDPR. The creation and maintenance of the electronic staff register concerns the processing of personal data.[21] Likewise, ordering the disclosure of such personal data in the context of civil proceedings is an instance of processing this data.[22] Thus, the situation in the main proceedings is within the material scope of the GDPR.

33. What does that mean for the operation of national procedural rules, such as the RB?

2. National law is the condition for the lawfulness of data processing by national courts

34. The legal basis for adopting the order for disclosure at issue in the present case is the RB.

35. The GDPR indeed requires that data processing in a situation such as the one in the present case has Member State (or EU) law as its legal basis.[23]

36. Originally collected and processed for tax purposes, under the order for disclosure in the present case, the data at issue are now to be processed for a probative purpose in judicial proceedings.

37. Article 6(4) of the GDPR allows for the repurposing of data processing if based on Member State law, which is a necessary measure in a democratic society to safeguard the objectives referred to in Article 23(1) of the GDPR. Among these objectives, Article 23(1)(f) lists 'the protection of judicial independence and judicial proceedings'.

38. All of the participants to this preliminary reference procedure agree that Article 23(1)(f) of the GDPR is the proper provision to rely on to justify the repurposing of data processing on the basis of the RB.[24]

39. The RB empowers national courts to order the disclosure of documents if they have probative value in a civil procedure. As explained, if a document to be disclosed contains personal data, the court ordering such a disclosure becomes the data controller under the GDPR.

40. As the Commission pointed out at the hearing, the national court is only to a certain extent an ordinary controller. Namely, national courts can only process data in the exercise of their official authority.

41. When data processing takes place in the exercise of official authority,[25] Article 6(3) of the GDPR requires it to be based on EU or Member State law.

[21] The Court has confirmed that records of working time in specific constitute personal data in the judgment of 30 May 2013, *Worten* (C-342/12, EU:C:2013:355, paragraph 19).

[22] The transmission of documents to the court in the context of civil proceedings was considered processing in the Opinion of Advocate General Campos Sánchez-Bordona in *Inspektor* v *Inspektorata kam Visshia sadeben savet (Purposes of the processing of personal data – Criminal investigation)* (C-180/21, EU:C:2022:406, points 82 and 83). At the moment of the publication of this Opinion, that case is still pending before the Court.

[23] In the context of Directive 2002/58, the Court considered that that directive does not preclude the possibility of Member States laying down an obligation to disclose personal data in the context of civil proceedings. See, to that effect, judgment of 29 January 2008, *Promusicae* (C-275/06, EU:C:2008:54, paragraph 53). To my mind, the same also applies to the GDPR.

[24] Additionally, the Commission proposed that another reason for justifying the repurposing of data processing in the present case could be found in Article 23(1)(i) of the GDPR ('the protection of the data subject or the rights and freedoms of others'). The Polish Government pointed to Article 23(1)(j) of the GDPR ('the enforcement of civil law claims').

[25] Processing in the exercise of official authority is made possible by Article 6(1)(e) of the GDPR.

42. Therefore, both Article 6(4) of the GDPR (allowing for repurposed processing), and Article 6(3) thereof (allowing the processing of data in the exercise of official authority), require the existence of national (or EU) law as the legal basis for processing. [26]

43. The RB empowering the court to adopt the order for disclosure is, thus, a necessary condition for the lawfulness of the processing at issue.

3. The GDPR complements national procedural rules

44. If the legal basis required by the GDPR exists, and the order which entails the processing of personal data is adopted in conformity with such Member State law, are the GDPR requirements for lawful processing satisfied?

45. In my view, the existence of a legal basis in national law, although necessary, is not sufficient for the order for disclosure to be in conformity with the GDPR.

46. The referring court explained that under the RB, in principle no account is taken of the private nature of information when making decisions about the disclosure of evidence. Courts are required to take into consideration the interests of the two opposing parties, but the law itself does not mention that the interests of data subjects play any role.

47. Is the RB incompatible with the GDPR for not explicitly obliging courts, when they become data controllers, to take the interests of data subjects into consideration when enacting decisions that may influence their personal data?

48. In my opinion, that is not the case. One must take into consideration that different national acts serving as legal bases for data processing were not adopted specifically in the implementation of the GDPR, but have their own purposes. Moreover, the GDPR is directly applicable in Member States' legal orders and does not require implementation. What is therefore important is that when national procedural rules and the GDPR meet, the former provides space for a simultaneous application of the latter.

49. At the hearing, the Swedish Government confirmed that the RB does not require, but it also does not prohibit, the courts from taking the interests of data subjects into consideration. It therefore does not preclude the direct application of the GDPR to the judicial procedure governed by that code.

50. National courts are therefore subject to domestic procedural rules and the GDPR in parallel, the latter complementing national rules if the procedural activities of the courts entail the processing of personal data.

51. To conclude, national legislation need not expressly refer to the GDPR or oblige courts to take into consideration the interests of data subjects. It suffices that such legislation allows for a complementary application of the GDPR. It is only if that were not the case that the national act would be contrary to the GDPR. The RB, however, seems to allow for a complementary application of the GDPR. [27]

[26] The processing can also be based on the data subject's consent. However, that is not the case here.

[27] In the division of competences between the Court and the courts of Member States in the preliminary ruling procedure, it is for the national court to decide whether that is indeed the case.

52. In answering the first question of the referring court, I therefore conclude that Article 6(3) and (4) of the GDPR imposes requirements on national procedural legislation relating to disclosure obligations, whenever this entails the processing of personal data. National procedural legislation cannot prevent, in such a case, that the interests of the data subjects be taken into consideration. Those interests will be safeguarded if national courts respect the rules of the GDPR when deciding on the disclosure of documentary evidence in an individual case.

C. The obligations of the national court concerning the interests of data subjects

53. As subjects of the GDPR, national courts as data controllers must take into consideration the interests of data subjects. How should those interests be taken into consideration when adopting a concrete decision concerning disclosure? That is the essence of the second question of the referring court.

1. Proportionality

54. The interests of data subjects will be protected when the processing of their personal data complies with Articles 5 and 6 of the GDPR.[28] To quote Advocate General Pikamäe, compliance with Articles 5 and 6 of the GDPR ensures the protection of the right to private and family life and the protection of personal data, as guaranteed by Articles 7 and 8 of the Charter, respectively.[29]

55. The legitimate aims of processing are listed in Article 6 of the GDPR.[30] As explained in the previous section of this Opinion, the processing in the case at hand pursues a lawful purpose, given that the court exercised its official authority when ordering disclosure based on the national law that serves to ensure the orderly conduct of judicial proceedings. However, both Article 6, as well as Article 5 of the GDPR, require not only a legitimate aim, but also that the specific processing is *necessary* for achieving that aim.

56. The GDPR therefore requires that the court undertake a proportionality analysis when determining whether the disclosure of personal data in a concrete situation is necessary for the probative purpose in judicial proceedings.[31]

57. In that respect, Article 6(4) of the GDPR requires that the national law on which the repurposed processing is based be a *necessary and proportionate measure* to safeguard one of the objectives listed in Article 23(1) of the GDPR, in this case the protection of judicial independence and judicial proceedings. Further, Article 6(3) of the GDPR requires that processing in the exercise of official authority be *necessary for the exercise of such official authority vested in the controller*.

[28] Judgments of 16 January 2019, *Deutsche Post* (C-496/17, EU:C:2019:26, paragraph 57), and 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). The Court previously concluded the same in relation to Directive 95/46. See, for instance, judgments of 20 May 2003, *Österreichischer Rundfunk and Others* (C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 65), and of 13 May 2014, *Google Spain and Google* (C-131/12, EU:C:2014:317, paragraph 71).

[29] Opinion of Advocate General Pikamäe in *Vyriausioji tarnybinės etikos komisija* (C-184/20, EU:C:2021:991, point 36).

[30] The Court found that the list of situations of lawful data processing in Article 6 of the GDPR is exhaustive and restrictive. See judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)* (C-439/19, EU:C:2021:504, paragraph 99). In the context of Directive 95/46, the Court took the same approach to lawfulness of processing in judgment of 4 May 2017, *Rīgas satiksme* (C-13/16, EU:C:2017:336, paragraph 25); and of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA* (C-708/18, EU:C:2019:1064, paragraphs 37 and 38).

[31] See also recital 39 of the GDPR, which states that: '… the personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. … Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.'

58. The national law which forms the basis for processing may *in abstracto* comply with the requirements of Article 6(3) and (4) of the GDPR. Still, the lawfulness of each individual processing (including a specific court order for disclosure) depends on the concrete balancing of all the interests involved, bearing in mind the legitimate aim for which disclosure is requested. [32] Only in such a way can the national court decide whether and to what extent the disclosure is necessary.

59. It is thus clear that the GDPR requires a proportionality analysis. Is the GDPR of any further assistance in answering which concrete steps the court must take in such an analysis?

2. Specific steps to be taken by the national court

60. The proportionality analysis, as explained, must be carried out in each individual case, taking into consideration all the interests involved. In situations such as the case at hand, the interests behind the disclosure must be weighed against the interference with the right to the protection of personal data. [33]

61. The interests behind disclosure reflect the right to effective judicial protection (Article 47 of the Charter). The interests of data subjects, with which the former right conflicts, reflect the right to private and family life (Article 7 of the Charter) and the right to protection of personal data (Article 8 of the Charter). It is these rights that need to be balanced in order to decide whether disclosure of personal data is necessary.

62. In what follows, I will offer certain suggestions concerning the specific steps the national court may be expected to take.

63. To begin with, it may always be presumed that data subjects who have not given their consent to the processing have an interest in restricting the processing of their personal data. That is thus the default starting position for the national court: to justify why this interest should be interfered with.

64. In my view, instructions for carrying out this assessment may be found in Article 5 of the GDPR, containing the principles that the data controller must respect when processing personal data.

65. In that respect, the data minimisation principle, from Article 5(1)(c) of the GDPR, is of cardinal importance. That requirement is, as stated by the Court, [34] an expression of proportionality. It requires that personal data be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

66. The first question to ask is, therefore, whether the data in the staff register held by Entral are adequate. They will be adequate for the purpose for which they are to be disclosed if they indeed show the number of working hours spent by the Fastec employees on the construction site.

[32] The Court explained that balancing depends on the specific circumstances of a particular case. See, in that respect, judgment of 4 May 2017, *Rīgas satiksme* (C-13/16, EU:C:2017:336, paragraph 31). See, also, judgment of 19 December 2020, *Asociația de Proprietari bloc M5A-ScaraA* (C-708/18, EU:C:2020:104, paragraph 32).

[33] See, by analogy, judgment of 9 November 2010, *Volker und Markus Schecke and Eifert* (C-92/09 and C-93/09, EU:C:2010:662, paragraph 77).

[34] Judgment of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)* (C-439/19, EU:C:2021:504, paragraph 98).

67. The second question is whether the data in the staff register held by Entral are relevant for the purpose for which they are requested. The purpose seems to be the interest of Nycander to prove its argument that Fastec employees worked for fewer hours than what is stated on the invoice. In such circumstances, the staff register would be relevant if it can indeed prove or disprove such a claim. The national court must assess its relevance in the light of other facts of the case (for example, the claim by Fastec that the staff register contains only a portion of the relevant working hours, others being spent outside the construction site).

68. In order to respond to the third requirement of data minimisation, the national court must determine whether all or only some of the data contained in the register are sufficient for probative purposes. In addition, if there are other ways to demonstrate the same fact, data minimisation requires that those other ways be used. For example, the national court might need to assess the claim by Fastec that the actual hours worked may be verified by reference to documents that already form part of the case file before the referring court. If it finds that claim to be true, the national court cannot order the disclosure of personal data in the staff register.

69. The national court needs to establish what types of personal data from the register are sufficient to prove or disprove the relevant facts. In that respect, the data minimisation principle requires that only data that are strictly necessary for the purpose in question be disclosed. It might therefore be necessary that Entral, as the processor, modifies the staff register in such a way that it limits the personal data to the necessary minimum, while allowing a conclusion to be drawn on the actual hours worked.

70. In that respect, the national court must determine whether it is necessary that persons whose data are in the register are identifiable for the disclosure to have probative value (for example, if it is necessary to name individual workers in order to invite them to stand as witnesses). Otherwise, it may be sufficient to have the information concerning the total number of hours spent on the construction site and/or the number of persons that worked those hours.

71. Depending on the answers to the foregoing questions, the court may decide to ask for the disclosure of pseudonymised or anonymised data. [35]

72. Under recital 26 of the GDPR, data that have undergone pseudonymisation remain within the material scope of the GDPR. That is so because it remains possible to trace the identity of a person behind the pseudonym. The opposite is true for anonymised data, which are outside its scope. The manner of disclosure ultimately ordered by the national court will therefore also have an effect on the further applicability of the GDPR. [36]

73. Ultimately, it will be for the national court to determine the probative value of different versions of the staff register in order to decide what type of data minimisation, if any, is necessary for the sound completion of the judicial proceedings before it.

74. Aside from the data minimisation principle in Article 5(1)(c) of the GDPR, other principles contained in Article 5 of the GDPR also bind the national court and are relevant for the method of adopting the order for disclosure.

[35] Fastec is indeed asking the referring court to either reject Nycander's request that the staff register be produced, or, in the alternative, that the staff register is produced only after anonymisation. The Commission, relying on the principle of data minimisation and referring to Article 25(1) of the GDPR, proposed that a solution might also be to produce a *pseudonymised* version of the staff register.

[36] For example, anonymising the register relieves the data controller of the obligation to inform the data subjects on the processing that would normally be required under Article 14 of the GDPR.

75. For example, Article 5(1)(a) of the GDPR, apart from referring to the principle of lawfulness (further elaborated in Article 6 thereof), also mentions the principle of transparency. To my mind, that principle demands that the national court clearly explains its decision to order the disclosure of personal data, by, inter alia, stating how it balanced the different interests and arguments of the parties relating to the disclosure.

76. Proper reasoning in the order for disclosure also satisfies the requirement of Article 5(2) of the GDPR, requiring that the data controller be able to demonstrate compliance with the principles stated in Article 5(1) thereof.

77. The manner of compliance with the principles of Article 5 of the GDPR can also be read from recital 31 of the GDPR. It requires that 'requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems'.

78. A concern relating to the proportionality assessment by the national court has been raised by the Polish Government: if the national court is to assess the probative value of the staff register or another piece of evidence in the proceedings before it, is it not already becoming too involved in what should remain the role of the parties, namely, attempting to win an argument concerning the very probative value of such evidence?

79. In my view, the assessment of the probative value, which takes into consideration the interests of data subjects, does not lead to more interference with the case than the assessment of probative value of any other evidence in civil proceedings. [37]

80. The level of the national court's interference will depend on the obviousness of the probative value of the data whose disclosure is being requested in the circumstances of the individual case. It will always pertain to the individual case to what extent the disclosure might interfere with the interests of data subjects.

81. For example, some cases may involve sensitive data with a special protection regime under Article 9 of the GDPR, or criminal sanctions data pertaining to the regime of Article 10 thereof. In such situations, the interests of data subjects will necessarily gain more weight in the balancing exercise. [38] Likewise, the interest in disclosure may differ across individual cases. While at times it will be clear that the relevance of the requested evidence is marginal, in other situations it will be central to the determination of the outcome of the case. In that respect, there is value to the Commission's point that the national court should enjoy broad discretion when making such assessments. Yet, it should never be relieved of the obligation to take into account the interests of data subjects.

82. The Czech Government voiced another concern: imposing obligations on national courts to take into consideration the interests of data subjects whenever they are ordering the disclosure of documentary evidence would hinder the regular operation of judicial proceedings. The GDPR

[37] As explained by the referring court, under the RB, courts are already bound to weigh the relevance of the evidence against the opposing party's interest in not releasing that information.

[38] In the context of Directive 2002/58, the Court has consistently held that the greater the extent of interference with the right to data protection, the more important the public interest objective pursued must be. Judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970, paragraph 115); of 2 October 2018, *Ministerio Fiscal* (C-207/16, EU:C:2018:788, paragraph 55); 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 131); and of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)* (C-746/18, EU:C:2021:152, paragraph 32).

indeed introduces an additional obligation [39] for courts to undertake the proportionality review before ordering disclosure of documentary evidence containing personal data. However, neither is the balancing of interests an unusual intellectual exercise for the courts to undertake, nor is the burden placed on national courts different from the one imposed on any data controller by the GDPR.

83. If the Union citizens are to enjoy a high level of protection of their personal data, consistent with the choice of the EU legislature as expressed in the GDPR, taking into consideration the interests of data subjects cannot be seen as an excessive burden placed on the Member States' courts.

84. I therefore propose that the Court answer the second question of the referring court as follows: when deciding on the order for disclosure in civil proceedings that entails the processing of personal data, the national court must undertake a proportionality analysis that takes into account the interests of data subjects whose personal data are to be processed and balance them in relation to the interest of the parties to the procedure to obtain evidence. That proportionality assessment is guided by the principles set out in Article 5 of the GDPR, including the principle of data minimisation.

V. Conclusion

85. In the light of the foregoing considerations, I propose that the Court answer the two questions referred for a preliminary ruling by the Högsta domstolen (Supreme Court, Sweden) as follows:

(1) Article 6(3) and (4) of the 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) imposes requirements on national procedural legislation relating to disclosure obligations whenever disclosure entails the processing of personal data. National procedural legislation cannot prevent, in such a case, that the interests of data subjects are taken into consideration. Those interests will be safeguarded if national courts respect the rules of Regulation 2016/679 when deciding on the disclosure of documentary evidence in an individual case.

(2) When deciding on the order for disclosure in civil proceedings that entails the processing of personal data, the national court must undertake a proportionality analysis that takes into account the interests of data subjects whose personal data are to be processed and balance them in relation to the interest of the parties to the procedure to obtain evidence. That proportionality assessment is guided by the principles set out in Article 5 of Regulation 2016/679, including the principle of data minimisation.

[39] In those legal systems whose procedural rules have not previously demanded such review.