Reports of Cases

OPINION OF ADVOCATE GENERAL
BOBEK
delivered on 26 January 2017 [1]

**Case C-13/16**

**Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde**
**v**
**Rīgas pašvaldības SIA 'Rīgas satiksme'**

**(Request for a preliminary ruling from the Augstākā tiesa, Administratīvo lietu departaments (Supreme Court, Administrative Division, Latvia))**

(Request for a preliminary ruling — Personal data — Lawful data processing — Article 7(f) of Directive 95/46/EC — Scope and conditions — Obligation or faculty to process personal data — Notion of processing necessary for the purposes of the legitimate interests pursued by the controller or by a third party)

## I. Introduction

1. A taxi driver stopped his vehicle at the side of the road in Riga. When a trolleybus belonging to Rīgas satiksme ('the Respondent') was passing by, a passenger in the taxi suddenly opened the door. A collision ensued, damaging the trolleybus. Rīgas satiksme asked the police ('the Appellant') to disclose the identity of the passenger. It wished to sue him for the damage caused to the trolleybus before the civil courts. The police gave Rīgas satiksme only the passenger's name. They refused to provide the ID number and address.

2. Against this factual background, the referring court asks whether Article 7(f) of Directive 95/46/EC ('the Directive') [2] imposes an obligation to disclose all the personal data necessary to launch civil proceedings against the person allegedly responsible for an administrative offence. It further questions whether the answer to the latter would vary if that person were a minor.

## II. Legal framework

### A. EU law

1. *Charter of Fundamental Rights of the European Union ('the Charter')*

3. Article 7 provides that 'everyone has the right to respect for his or her private and family life, home and communications'.

1 — Original language: English.

2 — 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).

4. By virtue of Article 8:

‘1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.’

2. *Treaty on the Functioning of the European Union*

5. Article 16(1) TFEU provides that ‘everyone has the right to the protection of personal data concerning them’.

3. *Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*

6. Article 2 lays down a number of definitions for the purposes of the Directive.

‘(a) “personal data” shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) “processing of personal data” (“processing”) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

…

(f) “third party” shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorised to process the data;

…’

7. Article 5, in Chapter II entitled ‘General rules on the lawfulness of the processing of personal data’, provides that ‘Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful’.

8. Article 6(1) reads as follows ‘Member States shall provide that personal data must be:

‘…

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

…’

9. Article 7 states that 'Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) 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; or

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

(d) processing is necessary in order to protect the vital interests of the data subject; or

(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 or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1(1).'

10. Article 8 prohibits, as a matter of principle, the processing of special categories of data, such as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs. However, it provides for a number of exceptions.

11. In particular, the prohibition does not apply, according to Article 8(2)(e), where 'the processing … is necessary for the establishment, exercise or defence of legal claims'.

12. Article 8(5) provides that:

'… Member States may provide that data relating to administrative sanctions or judgments in civil cases shall also be processed under the control of official authority.'

13. According to Article 8(7), 'Member States shall determine the conditions under which a national identification number or any other identifier of general application may be processed'.

14. Pursuant to Article 14, 'Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

…'

15. The Directive has now been repealed by Regulation (EU) 2016/679.[3] It entered into force on 24 May 2016. However, the new Regulation will only be applicable from 25 May 2018.

3 — Regulation 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).

## B. National law

16. Article 7 of the Fizisko personu datu aizsardzības likums (Law on the protection of personal data) is drafted in similar terms to Article 7 of the Directive. It provides that the processing of personal data is to be authorised, save if otherwise provided by law, only if at least one of the following requirements is met:

(1) the data subject has given his consent;

(2) 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;

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

(4) processing is necessary in order to protect the vital interests of the data subject, including his life and health;

(5) 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 data controller or in a third party to whom the data are disclosed;

(6) processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

## III. The dispute in the main proceedings and the question referred to the Court

17. In December 2012, a road accident occurred in Riga. A taxi driver had stopped his vehicle at the side of the road. As a trolleybus belonging to Rīgas satiksme was passing alongside the taxi, the taxi passenger opened the door, which scraped against and damaged the trolleybus. Administrative proceedings were initiated as a result of the accident. A report was drawn up, finding that an administrative offence had occurred.

18. Initially, because it considered that the taxi driver was responsible for that accident, Rīgas satiksme sought compensation from the insurance company covering the civil liability of the owner of the taxi. However, the insurance company informed Rīgas satiksme that it would not pay any compensation, as the accident was not attributable to the taxi driver, but rather to the passenger, against whom Rīgas satiksme could bring civil proceedings.

19. Rīgas satiksme applied to the Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvaldes Satiksmes administratīvo pārkāpumu izskatīšanas birojs (Office responsible for road traffic administrative infringements of the Security Police of the Region of Riga) ('the police'). It asked for information concerning the person on whom an administrative penalty had been imposed in respect of the accident. More specifically, it requested the name, identity document number, and address of the taxi passenger, as well as copies of the documents containing the explanations given by the taxi driver and the passenger on the circumstances of the accident. Rīgas satiksme indicated to the police that the information requested would be used only for the purpose of initiating civil proceedings against that person.

20. The police granted Rīgas satiksme's request only in part. It provided only the name of the taxi passenger. It refused to provide the identity document number and the address of that person. Nor did it provide Rīgas satiksme with the explanations given by the persons involved in the accident.

21. In its decision, the police stated that documents in the case file in administrative proceedings leading to sanctions may be provided only to the parties to those proceedings. Rīgas satiksme was not such a party. Moreover, as regards the identity document number and the address, the Datu valsts inspekcija (Latvian Data Protection Agency) prohibits the provision of such information relating to individuals.

22. In accordance with Article 261 of the Latvijas Administratīvo pārkāpumu kodekss (Latvian Administrative Infringements Code), in administrative proceedings leading to sanctions, a person may at his express request be given the status of victim. Rīgas satiksme did not exercise its right to have the status of victim in the administrative proceedings in question.

23. Rīgas satiksme commenced administrative proceedings against the decision of the police in so far as it refused to reveal the identity document number and address of the taxi passenger.

24. By judgment of 16 May 2014, the Administratīvā rajona tiesa (District Administrative Court) upheld the action brought by Rīgas satiksme. It ordered the police to provide the information requested in the application, namely the identity document number and the address of the taxi passenger.

25. The police appealed against that ruling before the Augstākā tiesa (Supreme Court, Latvia), the referring court in this case. The referring court first sought an opinion from the Latvian Data Protection Agency. The latter indicated that, in this specific case, the data could not be provided on the basis of Article 7(6) of the Law on the protection of personal data, given that the Administrative Infringements Code sets out the natural or legal persons to which or to whom the police may send information relating to a case. Thus, the disclosure of personal data relating to administrative proceedings leading to sanctions may be carried out only in accordance with paragraphs 3 and 5 of that article. In addition, Article 7 of that law does not *oblige* the data controller (in this case, the police) to process the data: it merely *permits* it to do so.

26. The Latvian Data Protection Agency also indicated that Rīgas satiksme had other means of obtaining the information: either by submitting a reasoned request to the Iedzīvotāju reģistrs (Civil Registry) or, pursuant to Articles 98, 99 and 100 of the Civilprocesa likums (Latvian Law on Civil Procedure), by applying to the courts for the production of evidence. The respective court can then order the police to disclose the personal data that Rīgas satiksme needs in order to be able to bring civil proceedings against the person concerned.

27. The referring court expresses doubts regarding the alternative means of obtaining the personal data referred to by the Latvian Data Protection Agency. If an application is made to the Civil Registry mentioning only the name of the taxi passenger, it may be that the name in question is shared by many people. Then, the relevant person may be identified only by means of additional data, such as those requested in the instant case (the identity document number and the address). Furthermore, the Latvian Data Protection Agency cited the provisions of the Law on Civil Procedure concerning the production of evidence. In accordance with Article 128 of the Law on Civil Procedure, upon submitting an application, it is necessary to indicate the name and identity document number (if known) of the defendant, as well as his legal domicile and the additional address indicated in the register, or, failing that, his address for service. Consequently, the applicant would have to know the place of residence of the defendant at the very least.

28. According to the referring court, the alternative means of obtaining the necessary personal data are therefore unclear or ineffective. As a consequence, in order to pursue its legitimate interests, it might be necessary for Rīgas satiksme to obtain the requested personal data from the police.

29. The referring court also conveys doubts as to the interpretation of the term 'necessary' in Article 7(f) and considers that that interpretation is decisive for the outcome of the present proceedings.

30. The Augstākās tiesas (Administratīvo lietu departaments) (Supreme Court (Administrative Division), Latvia) therefore decided to stay its proceedings and refer the following questions to the Court of Justice for a preliminary ruling:

'Must the phrase "is necessary for the purposes of the legitimate interests pursued by the … third party or parties to whom the data are disclosed", in Article 7(f) of 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, be interpreted as meaning that the National Police must disclose to Rīgas satiksme the personal data sought by the latter which are necessary in order for civil proceedings to be initiated? Is the fact that, as the documents in the case file indicate, the taxi passenger whose data is sought by the Rīgas satiksme was a minor at the time of the accident relevant to the answer to that question?'

31. Written observations were submitted by Rīgas satiksme, the Commission, and the Czech, Spanish, Latvian, Austrian, and Portuguese Governments. The Commission and the Latvian Government presented oral argument at the hearing that took place on 24 November 2016.

## IV. Assessment

32. The referring court essentially asks whether there is, under the Directive, a *duty* on the part of the controller of the data to disclose data enabling the identification of a person allegedly responsible for an administrative offence so that Rīgas satiksme can launch civil proceedings.

33. My concise answer to that specific question asked by the referring court is 'no'. The Directive itself does not establish any such obligation. It merely provides a faculty (in the sense of permission or authorisation) to do so, as long as a number of elements are united. The *faculty* of carrying out certain activity under law is a distinct category from the *obligation* to carry out that activity.

34. However, on the facts of this case, the issue does not end there. At least in part, that is, in relation to the information that has been effectively provided, the Court is also called upon to determine the conditions for the application of Article 7(f) of the Directive and the nature and scope of personal data that a data requester may obtain in application of that provision.

35. This Opinion is therefore structured as follows: first, I will articulate why, in my view, no obligation to disclose on the part of the entity in possession of the information arises from the Directive (Section A). Second, in order to provide the referring court with a full and useful answer in the present case, I will propose conditions for the application of Article 7(f) of the Directive and the scope of personal data that may be disclosed if the conditions are met (Section B).

### *A.* Obligation to disclose

36. The referring court asks whether personal data *must* be disclosed for the purposes of initiating civil proceedings *by virtueof* Article 7(f) of the Directive. In other words, the referring court asks whether the Directive itself imposes a duty to disclose that personal data.

37. In my view, no such obligation can be inferred from the Directive itself. That unequivocally follows from the text and the system, as well as the very purpose of the Directive.

38. Starting with the system and logic of the Directive, the default rule underpinning that directive is that personal data should, in general, *not* be processed, so that a high level of protection of the right to privacy is ensured.[4] The processing of personal data shall, by nature, remain rather exceptional.

39. Article 7 is placed within this system. That article sets out a list of exceptions to the default rule, whereby processing is legitimate certain strictly articulated conditions. Thus, the categories of Article 7 are the exceptions to the overall rule.

40. Against this background, the text of Article 7 clearly confirms that the categories listed are to be treated as a mere faculty or possibility to process personal data, as opposed to an obligation, when the factual situation falls within one of the legal exceptions. According to that provision, 'Member States shall provide that personal data *may* be processed *onlyif* …'.[5] That language, which is also used in the other linguistic versions,[6] clearly shows that Article 7 exceptions are indeed exceptions. They cannot be construed as an obligation to process personal data.

41. The fact that at least some of the Article 7 exceptions have direct effect[7] does not alter the previous conclusion. They do not create, per se, a right to obtain information for those who ask for it, nor do they create a corollary obligation for those in possession thereof to disclose it. Article 7 rather provides for general rules in order for the data processor to determine when, if, how and to what extent it *may* process personal data that it has acquired.

42. Finally, the overall purpose of the Directive is to provide common EU boundaries or limits to the processing of personal data. The concrete individual grounds and reasons for the processing will then typically be found in national law, or in other EU legal instruments. In other words, the Directive provides the limits to, not the instigation of, data processing.

43. Thus, the text, system, logic and purpose of the Directive are all quite clear in indicating that Article 7(f) of the Directive cannot be read as providing, in and of itself, for an *obligation* to disclose personal data.

44. On a broader systematic and subsidiary note, it might also be added that a similar structure is in no way uncommon in other areas of EU law in which EU secondary law instruments directly or indirectly touch upon personal data.

45. For example, Directive 2002/58/EC on privacy and electronic communication,[8] which complements Directive 95/46 with regard to the electronic communication sector, also does not contain an obligation of disclosure. The Court made clear in *Promusicae* that the former does not preclude the Member States from laying down an obligation to disclose personal data in the context of civil proceedings, nor compel them to do so.[9] It is therefore for the Member States to decide. It is not a necessary consequence of EU law.

4 — See, for example, judgments of 24 November 2011, *Asociación Nacional de Establecimientos Financieros de Crédito* (C-468/10 and C-469/10, EU:C:2011:777, paragraph 25), and of 13 May 2014, *Google Spain and Google* (C-131/12, EU:C:2014:317, paragraph 66).

5 — Emphasis added.

6 — For example, in French, '… le traitement de données à caractère personnel ne peut être effectué que si …'; in German, '… die Verarbeitung personenbezogener Daten lediglich erfolgen darf …'; in Italian, '… il trattamento dei dati personali può essere effettuato soltanto quando …'; in Spanish, '… el tratamiento de datos personales sólo pueda efectuarse si …'; in Czech, ' … zpracování osobních údajů může být provedeno pouze pokud …'.

7 — See, for Article 7(f), judgment of 24 November 2011, *Asociación Nacional de Establecimientos Financieros de Crédito* (C-468/10 and C-469/10, EU:C:2011:777, paragraph 52); for Article 7(c) and Article 7(e), judgment of 20 May 2003, *Österreichischer Rundfunk and Others* (C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraphs 99 to 101).

8 — Directive 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 (OJ 2002 L 201, p. 37).

9 — See judgment of 29 January 2008 (C-275/06, EU:C:2008:54, paragraphs 54 to 55).

46. Similarly, the Court has held that other directives,[10] which touch upon personal data but mainly aim at ensuring effective protection of intellectual property in the information society,[11] also did not require the Member States to lay down an obligation to provide personal data in order to ensure the effective protection of copyright in the context of civil proceedings.[12]

B. Faculty to disclose

47. As stated by the referring court, the Respondent effectively received *some* personal data: the name and the surname of the person concerned. The remainder of its request was denied. This must presumably have happened on the basis of national law.

48. Therefore, and with regard to the personal data effectively disclosed, the question of whether or not that disclosure was compatible with Article 7 of the Directive is of relevance.

49. It ought, however, to be clearly stressed that the following part of this Opinion relates to the *faculty* to disclose personal data in a factual situation such as the one in the main proceedings, *on the condition* that national law provides the legal basis for such disclosure. In other words, what limits does EU law set for disclosure of personal data in such a situation? If national law provided for the disclosure of personal data in a similar situation, would such a disclosure be compatible with Article 7(f) of the Directive?

50. In my view, in a situation such as that in the main proceedings, it is fully compatible with Article 7(f) to provide personal data to the scope and degree that would enable an injured party to commence civil proceedings.

51. In this section therefore, I first examine the appropriate legal basis for processing personal data under the Directive in a similar factual situation. Second, I propose conditions for the application of Article 7(f) of the Directive. Third, I assess the present case in the light of those conditions.

1. The appropriate legal basis under Article 7 of the Directive

52. A preliminary issue, discussed in both the written and oral submissions, is which subparagraph of Article 7 of the Directive ought to be applicable in a factual situation such as that in the main proceedings.

53. Most of the parties and interveners relied on Article 7(f), invoked by the referring court. However, the Austrian Government argued in its written submissions that Article 7(f) of the Directive is not the correct legal basis, even for the purposes of issuing civil proceedings. This is because it allegedly sets out too abstract and imprecise a ground for data processing. It cannot therefore justify such an interference with the right to data protection.

54. In its written submissions, the Commission focused on Article 7(f). In its oral submissions, however, it also suggested that data processing such as that in the main proceedings could also fall under Article 7(c) or Article 7(e) of the Directive.

10 — See Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (OJ 2000 L 178, p. 1); Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ 2001 L 167, p. 10); Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ 2004 L 157, p. 45).

11 — The Court insisted in particular on the fact that the protection of industrial property that is ensured by those directives cannot affect the requirements of the protection of personal data and, also, on the need to reconcile the requirements of the protection of different fundamental rights: see judgment of 29 January 2008, *Promusicae* (C-275/06, EU:C:2008:54, paragraphs 57 and 65).

12 — See judgment of 29 January 2008, *Promusicae* (C-275/06, EU:C:2008:54, paragraph 70).

55. Article 7 of the Directive sets out different legal bases for lawful data processing by distinguishing between six scenarios. In order for those data to be processed, they need to fall under at least one of the categories in Article 7. However, it is clear that the scope and rationale of these provisions are distinct.

56. In broader, abstract terms, Article 7 contains three types of exceptions, for which the processing of personal data shall be lawful: first, when the data subject has given his or her consent (Article 7(a)); second, when legitimate interests of the controller or of third parties are to some extent presumed (Article 7(b) to (e)); and third, when competing legitimate interests need not only to be established, but also to outweigh the interests or rights and freedoms of the data subject (Article 7(f)).

57. Thus, the scope of Article 7(f) is admittedly broader than that of Article 7(c) or Article 7(e). The **former** is not bound to specific legal or factual circumstances, but is framed in quite general terms. However, its application is more stringent since it is conditional on the actual existence of legitimate interests of the controller or of a third party that outweigh those of the data subject, which is not required for Article 7(c) or Article 7(e).

58. However, academic discussions aside, two points are worth highlighting. First, the Article 7 exceptions are not mutually exclusive. Thus, two or potentially all three might be applicable to one set of facts.[13] Second, in spite of somewhat different wording, the practical difference in application is likely to be rather minimal, provided that there is a clearly articulated and credible legitimate interest.

59. With these caveats in mind, but deferring to the national court — which has full knowledge of the facts of the case and national law as presented in its question and invokes Article 7(f) of the Directive as being the applicable exception — I believe that the Court should proceed on that basis.

## 2. The conditions and scope of Article 7(f) of the Directive

60. Article 7(f) contains two cumulative conditions. Both must be fulfilled in order for the processing of personal data to be lawful: firstly, the processing of the personal data must be *necessary* for the purposes of the *legitimate interests* pursued by the controller or by the third party or parties to whom the data are disclosed. Secondly, such interests must *not be overridden* by the fundamental rights and freedoms of the data subject.[14]

61. The second condition aims at the balancing of the interests involved. The first one can actually be split into two sub-conditions for didactical purposes: the legitimate interest itself, on the one hand, and the necessary character of processing, that is, a type of proportionality, on the other.

62. Thus, three elements must be present for the purposes of Article 7(f): the existence of a legitimate interest justifying processing (a); the prevalence of that interest over the rights and interests of the data subject (balancing of interests) (b); and the necessity of processing for the realisation of the legitimate interests (c).

### (a) Legitimate interest

63. First, processing under Article 7(f) of the Directive is conditional upon the existence of legitimate interests of the data controller or of a third party.

13 — Regulation No 2016/679 is even more explicit in this respect. Article 6(1), which replaces Article 7 of the Directive, states that 'Processing shall be lawful only if and to the extent that *at least one* of the following applies …' (emphasis added).

14 — See judgment of 24 November 2011, *Asociación Nacional de Establecimientos Financieros de Crédito* (C-468/10 and C-469/10, EU:C:2011:777, paragraph 38).

64. The Directive does not define legitimate interests.[15] Thus, it is for the data controller or processor, under the supervision of national courts, to determine whether there is a legitimate aim that could justify an interference with private life.

65. The Court has already held that transparency[16] or the protection of the property, health and family life[17] are legitimate interests. The notion of legitimate interests is elastic enough to accommodate other kinds of considerations. There is no doubt in my mind that the interest of a third party in obtaining the personal information of a person who damaged their property in order to sue that person for damages can be qualified as a legitimate interest.

(b) Balancing of interests

66. The second condition relates to balancing between two sets of competing interests, namely the interests and rights of the data subject[18] and the interests of the controller or of third parties. The balancing requirement clearly results both from Article 7(f) and from the legislative history of the Directive. As to the text of the latter, Article 7(f) requires that the legitimate interests of the data subject him or herself be balanced against the legitimate interests of the controller or of a third party. The legislative history confirms that the balancing of interests was already provided for, in slightly different ways, in the Commission's initial proposal[19] and also in its amended proposal after the first reading of the European Parliament.[20]

67. The Court has held that application of Article 7(f) necessitates a balancing of the opposing rights and interests concerned. Account must be taken of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter.[21] Such an act of balancing must be carried out on a case-by-case basis.[22]

68. Balancing is the key to the correct application of Article 7(f). It is that operation that makes Article 7(f) wholly distinctive compared to the other provisions of Article 7. It is always dependent on the circumstances of the individual case. It is for these reasons that the Court has stressed that Member States cannot definitively prescribe, for certain categories of personal data, the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of the particular circumstances of an individual case.[23]

15 — See Opinion 06/2014 of Article 29 Data Protection Working Party on the 'Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC' (844/14/EN WP 217).

16 — Judgment of 9 November 2010, *Volker und Markus Schecke and Eifert* (C-92/09 and C-93/09, EU:C:2010:662, paragraph 77).

17 — Judgment of 11 December 2014, *Ryneš* (C-212/13, EU:C:2014:2428, paragraph 34).

18 — Several provisions of the Directive aim at protecting the data subject, whether in terms of information to be given to him or her (Articles 10 and 11) or in terms of access to his or her own data (Article 12). Article 14 specifically provides for the data subject's right, 'at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him'.

19 — Proposal for a Council Directive concerning the protection of individuals in relation to the processing of data (COM(90) 314 final).

20 — Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (COM(92) 422 final).

21 — Judgments of 24 November 2011, *Asociación Nacional de Establecimientos Financieros de Crédito* (C-468/10 and C-469/10, EU:C:2011:777, paragraphs 38 and 40), and of 13 May 2014, *Google Spain and Google* (C-131/12, EU:C:2014:317, paragraph 74).

22 — Judgment of 24 November 2011, *Asociación Nacional de Establecimientos Financieros de Crédito* (C-468/10 and C-469/10, EU:C:2011:777, paragraph 40).

23 — Judgments of 24 November 2011, *Asociación Nacional de Establecimientos Financieros de Crédito* (C-468/10 and C-469/10, EU:C:2011:777, paragraph 47), and of 19 October 2016, *Breyer* (C-582/14, EU:C:2016:779, paragraph 62).

69. In order to meaningfully carry out that balancing, due consideration should in particular be given to the nature and sensitivity of the data requested, their degree of publicity,[24] and the gravity of the offence committed. One of the potential elements to be weighed in the balancing exercise, which is of relevance for the present case, is the age of the data subject.

(c) Necessity

70. As far as necessity or, in a way, basic proportionality is concerned, the Court has held in general that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.[25] Therefore, the nature and amount of data that may be processed shall not go beyond what is necessary for the purposes of the legitimate interests at issue.

71. The examination of proportionality is an assessment of the relationship between aims and chosen means. The chosen means cannot go beyond what is needed. That logic, however, also works in the opposite direction: the means *must be capable* of achieving the stated aim.

72. In practical terms, the data controller, faced with the assessment of necessity, has two options. Either it refrains from disclosing *any* information, or, if it decides to process that information, then it must give *all the necessary* information for the purposes of the attainment of the legitimate interests at issue.[26]

73. First, Article 6(1)(c) and recital 28 of the Directive require that personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected, but also when further processed.[27] Thus, it follows from those provisions that the data disclosed shall also be *adequate and relevant* for the realisation of legitimate interests.

74. Second, common sense calls for a reasonable approach as to the data that should actually be processed. Data requesters should indeed be given useful and relevant information, which are necessary *and* sufficient for them to fulfil their own legitimate interests, without having to forward a request to another entity that might also possess that information.

75. Put metaphorically, the application of the criterion of necessity shall not turn the realisation of a legitimate interest into a Kafkaesque treasure hunt, strongly resembling an episode of *Fort Boyard*, in which the participants are sent from one room to another to collect partial clues to eventually work out where they are supposed to go.

76. Finally, it ought to be repeated that the precise scope of the data to be disclosed is a matter of national law. Admittedly, national law could also provide only for such partial disclosure, which in itself would be insufficient. That is indeed possible. The fact that national legislation seems to make little practical sense does not render it automatically incompatible with EU law, provided that that legislation remains within the regulatory space pertaining to the Member States. All that is suggested here is that Article 7(f) of the Directive is *not opposed* to full disclosure of all the necessary information that is needed to effectively pursue one's legitimate aim, as long as the other conditions are met.

24 — Judgment of 24 November 2011, *Asociación Nacional de Establecimientos Financieros de Crédito* (C-468/10 and C-469/10, EU:C:2011:777, paragraph 44).

25 — Judgments of 9 November 2010, *Volker und Markus Schecke and Eifert* (C-92/09 and C-93/09, EU:C:2010:662, paragraph 86), and of 11 December 2014, *Ryneš* (C-212/13, EU:C:2014:2428, paragraph 28).

26 — Logically, these two options will also be available when data are processed on the basis of any other ground laid down in Article 7.

27 — The Court has held that Article 6(1)(c) has direct effect (judgment of 20 May 2003, *Österreichischer Rundfunk and Others* (C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraphs 99 to 101).

3. Application to the present case

77. Having set out the overall framework of analysis, I shall now turn to the present case, with the caveat that it is naturally ultimately for the national court, given its detailed knowledge of the facts and national law, to come to a decision.

78. Rīgas satiksme requested that the police give them the taxi passenger's address and the identity document number in order to launch civil proceedings to obtain damages for the loss it suffered.

79. First, as rightly argued by the Czech, Spanish and Portuguese Governments, the issuing of a legal claim, as in the main proceedings, is a legitimate interest, as stated by Article 7(f).

80. This is also confirmed by Article 8(2)(e) of the Directive, which provides for the possible processing of certain sensitive data 'where the processing relates to data which are … necessary for the establishment, exercise or defence of legal claims'. If the exercise of a legal claim can justify the processing of sensitive data under Article 8, I fail to see why it could not a fortiori be seen as a legitimate interest justifying the processing of non-sensitive data under Article 7(f). That interpretation also follows from a pragmatic approach to the Directive in the light of the other secondary law instruments (mentioned above) that seek a balance between privacy and effective judicial protection. [28]

81. Second, with regard to the balancing of interests, in general, I see no reason why the interests for fundamental rights of the data subject should override the specific legitimate aim of the damaged party in pursuing civil proceedings. It is perhaps also worth adding in this context that all that the Respondent is asking for in fact is the possibility to begin legal proceedings before a civil court. The disclosure in itself would therefore not even bring about any immediate change to the legal situation of the data subject.

82. However, as rightly submitted by the Portuguese Government, it is at this balancing stage in particular that the age of the data subject ought to be taken into consideration.

83. The referring court indeed asks to what extent the fact that the taxi passenger was a minor at the time of the accident is relevant. To my mind, and given the particular circumstances of this case, it is not.

84. In general, the fact that the data subject is a minor is a factor that should indeed be taken into consideration in carrying out the balancing of interests. However, the special considerations owed to, and the enhanced protection of minor children should have a discernible connection to the type of data processing in question. Unless it is established precisely how the disclosure in this particular case were to endanger, for example, the physical or mental development of a child, I fail to see why the fact that the damage was caused by a minor should effectively lead to immunity from civil liability.

85. Finally, should the balancing of interests lead to the result that the interests of the data subject do not prevail over the interests of the person requesting disclosure of personal data, the final issue then arises: one of necessity and the scope of the information to be disclosed.

86. Again, it is for the referring court to identify the legal basis in national law which warrants such a disclosure. Once such a basis is identified, the 'necessity' criterion in Article 7(f) of the Directive is certainly not opposed, in my view, to the full disclosure of all the information needed to launch civil proceedings under Latvian law.

28 — See point 46 of this Opinion and footnotes 10 to 12.

87. The Latvian Government argued that, according to established case-law, the protection of the fundamental right to privacy requires that the derogations to the protection of personal data and the limitations thereto should be limited to what is strictly necessary. Although it acknowledged that alternative methods were available in order to obtain further data, it conceded that the name and surname were probably insufficient to exercise a legal claim and therefore it referred the assessment to the national court.

88. It should be noted that Article 8(7) of the Directive gives the Member States leeway to decide whether to disclose identification numbers. Member States shall not therefore be obliged to process identification numbers, unless it is absolutely necessary for bringing civil proceedings.

89. Irrespective of their precise nature, what matters is possession of all the relevant data that are indispensable for issuing a legal claim. Thus, if the address suffices under national law, then no further information should be disclosed.

90. It is for the national court to determine the amount of personal data that is necessary for Rīgas satiksme to effectively commence a legal action [29] under Latvian law. I merely wish to stress that, as already set out above in points 74 to 75 of this Opinion, the existence of alternatives to obtain the necessary personal data is not relevant for the application of Article 7(f). Rīgas satiksme ought to be able to get all the *necessary* information from the one controller to whom it applied.

## C. A data protection protective epilogue

91. This is a somewhat peculiar case. The referring court essentially enquires whether or not an exception *permitting* the processing of personal data can be interpreted as an *obligation* incumbent upon the data controller to disclose the identity of a person who caused a car accident. It would appear that the genuine reason for asking that question is that, at the national level, the avenues for obtaining such information have been made difficult, if not blocked entirely in the name of data protection.

92. Looking at the series of events in question, an uninformed bystander might raise the innocent question: should the issue of an individual request for the identity of a person who damaged that individual's property and whom the individual wishes to sue for damages really be a case in which the police officers are obliged to carry out several layers of balancing of interests and proportionality, followed by a protracted litigation, and an opinion from the national data protection authority?

93. The present case is yet another instance [30] in which data protection laws reach into and are employed in rather surprising circumstances. It generates, not just for the uninformed bystander, a certain intellectual unease as to the reasonable use and function of data protection rules. I will take this opportunity to make few concluding remarks in this regard.

94. There is no doubt that the protection of personal data is of primordial importance in the digital age. The Court has been at the forefront of the development of the case-law in this area, [31] and rightly so.

29 — Judgments of 14 September 2000, *Fisher* (C-369/98, EU:C:2000:443, paragraph 38); and of 16 December 2008, *Huber* (C-524/06, EU:C:2008:724, paragraph 67).

30 — Of the more recent case-law of this Court, see, for instance, judgment of 11 December 2014, *Ryneš* (C-212/13, EU:C:2014:2428). See also, although primarily concerned with other provisions of EU law, order of 11 January 2017, *Boudjellal*, (C-508/16,EU:C:2017:6).

31 — See, in particular, judgments of 8 April 2014, *Digital Rights Ireland and Others* (C-293/12 and C-594/12, EU:C:2014:238); and of 13 May 2014, *Google Spain and Google* (C-131/12, EU:C:2014:317; and of 6 October 2015, *Schrems* (C-362/14, EU:C:2015:650).

95. However, the cited cases truly reflect the main concern of personal data protection, for which it has been originally introduced and must be vigorously protected: *large-scale* processing of personal data by *mechanical*, digital means, in all its varieties, such as the compiling, administration, and the use of large datasets, passing on of datasets for purposes other than legitimate ones, assembling and harvesting of metadata, and so on.

96. As in any other area of law, rules governing certain activity must be sufficiently flexible in order to catch all the potential eventualities that arise. That might, however, lead to the danger of an overbroad interpretation and application of those rules. They might end up being applied also to a situation where the link with the original purpose is somewhat tenuous and questionable. Eventually, the overbroad application and certain 'application absolutism' might result in discrediting the original idea too, which was in itself very important and legitimate.

97. Generally speaking, in *Promusicae*, the Court insisted on the need to interpret the directives touching upon personal data so as to allow a fair balance to be struck between the various fundamental rights protected by the EU legal order.[32]

98. To this perhaps, a certain rule of reason could also be added, which ought to be employed at the stage of the balancing exercise. This would mean keeping the original and *primary* (certainly, by no means unique, simply primary) purpose of the legislation in mind: to regulate operations on a *largerscale* carried out by *mechanical*, automated means, and the use and transfer of information obtained from it. By contrast, a much lighter touch is, in my humble opinion, called for in situations when a person is asking for an *individual* piece of information relating to a specific person in a *concretised* relationship, when there is a clear and entirely legitimate purpose resulting from normal operation of the law.

99. In sum, common sense is not a source of law. But it certainly ought to guide interpretation of it. It would be most unfortunate if *protection* of personal data were to disintegrate into *obstruction* by personal data.

## V. **Conclusion**

100. In the light of the foregoing considerations, I recommend that the Court answer the question referred to it by the Augstākā tiesa, Administratīvo lietu departaments (Supreme Court, Administrative Division, Latvia) as follows:

Article 7(f) of 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 cannot be interpreted as establishing an obligation for the controller to disclose the personal data sought by a third party in order for civil proceedings to be initiated.

Article 7(f) of the Directive does not, however, oppose such disclosure, provided that national law foresees the disclosure of personal data in situations such as the one in the main proceedings. The fact that the data subject was a minor at the time of the accident is not material in this regard.

32 — Judgment of 29 January 2008, *Promusicae* (C-275/06, EU:C:2008:54, paragraph 68).