Reports of Cases

OPINION OF ADVOCATE GENERAL
SZPUNAR
delivered on 17 December 2020[1]

Case C-439/19

B
joined parties:
Latvijas Republikas Saeima

(Request for a preliminary ruling from the Satversmes tiesa (Constitutional Court, Latvia))

(Request for a preliminary ruling – Regulation (EU) 2016/679 – Processing of personal data – Information relating to penalty points for road traffic offences – Concept of processing of personal data relating to criminal convictions and offences – National rules providing for the disclosure of such information and allowing its re-use)

I. Introduction

1. In 1946, George Orwell commented on the 'Keep Death off the Roads' campaign, which a former Member State of the European Union was running at the time, as follows: 'If you really want to keep death off the roads, you would have to replan the whole road system in such a way as to make collisions impossible. Think out what this means (it would involve, for example, pulling down and rebuilding the whole of London), and you can see that it is quite beyond the power of any nation at this moment. Short of that you can only take palliative measures, which ultimately boil down to making people more careful'.[2]

2. The case at issue before the Satversmes tiesa (Constitutional Court, Latvia), which has turned to the Court by way of the present request for a preliminary ruling, has, at its core, the 'palliative measures' referred to above: in order to foster road safety by making drivers more aware and careful, penalty points are recorded against drivers who commit motoring offences. That information is then communicated and transmitted for re-use. The referring court, which is hearing a constitutional complaint that has been brought before it, is seeking to assess the compatibility of the national law in question with Regulation (EU) 2016/679[3] ('the GDPR').

3. This makes the present case an almost classic data protection case in the sense that it is predominantly set in the offline-world and involves a vertical relationship between a State and an individual, placing it seamlessly within a line of cases which have reached the Court since the seminal *Stauder* judgment,[4] arguably the first case on data protection *au sens large*.[5]

1 Original language: English.

2 See *Tribune* of 8 November 1946.

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).

4 See judgment of 12 November 1969 (29/69, EU:C:1969:57, paragraph 7).

5 And certainly the first case on fundamental rights in the EU legal order.

4. In assessing how far a Member State can interfere with the personal rights of an individual in order to pursue its aim of fostering road safety, I shall propose to the Court that measures such as the Latvian legislation in question are not proportionate to the aim they intend to achieve.

5. But before we get to that point, the present case raises a whole range of fundamental and intricate questions, which will take us through the GDPR at breakneck speed. Fasten your seatbelts. It may save you the odd penalty point.

II. Legal framework

A. EU law

1. The GDPR

6. Chapter I of the GDPR, entitled 'General Provisions', contains Articles 1 to 4, which set out the subject matter and objectives, material and territorial scope as well as definitions.

7. Article 1 of the GDPR, entitled 'Subject matter and objectives', reads as follow:

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

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

3. The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.'

8. Article 2 of the GDPR, entitled 'Material scope', provides:

'1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. 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.

...'

9. Chapter II of the GDPR, which contains Articles 5 to 11, sets out the principles of the regulation: principles relating to processing of personal data, lawfulness of processing, conditions for consent, including a child's consent in relation to information society services, processing of special categories of personal data and of personal data relating to criminal convictions and offences, and processing which does not require identification.

10. Pursuant to Article 5 of the GDPR, headed 'Principles relating to processing of personal data':

'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 insofar 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").'

11. Article 10 of the GDPR, headed 'Processing of personal data relating to criminal convictions and offences', states:

'Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.'

2. Directive 2003/98/EC

12. Article 1 of Directive 2003/98/EC,[6] headed 'Subject matter and scope', reads as follows:

'1. This Directive establishes a minimum set of rules governing the re-use and the practical means of facilitating re-use of existing documents held by public sector bodies of the Member States.

2. This Directive shall not apply to:

(a) documents the supply of which is an activity falling outside the scope of the public task of the public sector bodies concerned as defined by law or by other binding rules in the Member State, or in the absence of such rules, as defined in line with common administrative practice in the Member State in question, provided that the scope of the public tasks is transparent and subject to review;

(b) documents for which third parties hold intellectual property rights;

(c) documents which are excluded from access by virtue of the access regimes in the Member States, including on the grounds of:

— the protection of national security (i.e. State security), defence, or public security,

— statistical confidentiality,

— commercial confidentiality (e.g. business, professional or company secrets);

(ca) documents access to which is restricted by virtue of the access regimes in the Member States, including cases whereby citizens or companies have to prove a particular interest to obtain access to documents;

(cb) parts of documents containing only logos, crests and insignia;

(cc) documents access to which is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data, and parts of documents accessible by virtue of those regimes which contain personal data the re-use of which has been defined by law as being incompatible with the law concerning the protection of individuals with regard to the processing of personal data;

(d) documents held by public service broadcasters and their subsidiaries, and by other bodies or their subsidiaries for the fulfilment of a public service broadcasting remit;

(e) documents held by educational and research establishments, including organisations established for the transfer of research results, schools and universities, except university libraries and

(f) documents held by cultural establishments other than libraries, museums and archives.

3. This Directive builds on and is without prejudice to access regimes in the Member States.

6 Directive of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information (OJ 2003 L 345, p. 90), as amended by Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 (OJ 2013 L 175, p. 1).

4. This Directive leaves intact and in no way affects the level of protection of individuals with regard to the processing of personal data under the provisions of Union and national law, and in particular does not alter the obligations and rights set out in Directive 95/46/EC. [7]

5. The obligations imposed by this Directive shall apply only insofar as they are compatible with the provisions of international agreements on the protection of intellectual property rights, in particular the Berne Convention [8] and the TRIPS Agreement.' [9]

13. Article 2 of Directive 2003/98, headed 'Definitions', reads as follow:

'For the purpose of this Directive the following definitions shall apply:

1. "public sector body" means the State, regional or local authorities, bodies governed by public law and associations formed by one or several such authorities or one or several such bodies governed by public law;

2. "body governed by public law" means any body:

   (a) established for the specific purpose of meeting needs in the general interest, not having an industrial or commercial character; and

   (b) having legal personality; and

   (c) financed, for the most part by the State, or regional or local authorities, or other bodies governed by public law; or subject to management supervision by those bodies; or having an administrative, managerial or supervisory board, more than half of whose members are appointed by the State, regional or local authorities or by other bodies governed by public law;

3. "document" means:

   (a) any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording);

   (b) any part of such content;

4. "re-use" means the use by persons or legal entities of documents held by public sector bodies, for commercial or non-commercial purposes other than the initial purpose within the public task for which the documents were produced. Exchange of documents between public sector bodies purely in pursuit of their public tasks does not constitute re-use;

5. "personal data" means data as defined in Article 2(a) of Directive 95/46/EC.

6. "machine-readable format" means a file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure;

7 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).

8 The Berne Convention for the Protection of Literary and Artistic Works Paris Act of 24 July 1971, as amended on 28 September 1979.

9 The TRIPS Agreement (Agreement on Trade-Related Aspects of Intellectual Property Rights) constitutes Annex 1C to the Agreement establishing the World Trade Organisation (WTO Agreement), approved on behalf of the Community, as regards matters within its competence, by Council Decision 94/800/EC of 22 December 1994 (OJ 1994 L 336, p. 1).

7. “open format” means a file format that is platform-independent and made available to the public without any restriction that impedes the re-use of documents;

8. “formal open standard” means a standard which has been laid down in written form, detailing specifications for the requirements on how to ensure software interoperability;

9. “university” means any public sector body that provides post-secondary-school higher education leading to academic degrees.’

14. Article 3 of Directive 2003/98, headed ‘General principle’, reads as follows:

‘1. Subject to paragraph 2 Member States shall ensure that documents to which this Directive applies in accordance with Article 1 shall be re-usable for commercial or non-commercial purposes in accordance with the conditions set out in Chapters III and IV.

2. For documents in which libraries, including university libraries, museums and archives hold intellectual property rights, Member States shall ensure that, where the re-use of such documents is allowed, these documents shall be re-usable for commercial or non-commercial purposes in accordance with the conditions set out in Chapters III and IV.’

B. Latvian law

15. Article 14^1 (2) of the Ceļu satiksmes likums (‘the Law on motoring’) [10] is worded as follows:

‘Information relating to a vehicle owned by a legal person, … to a person’s right to drive vehicles, to fines for the commission of motoring offences which have been imposed on a person but not paid within the time limits laid down by law and other information recorded in the national register of vehicles and their drivers [“the national vehicle register”], as well as in the system of information on means of traction and drivers, shall be regarded as information in the public domain.’

III. Facts, procedure and questions referred

16. B, the applicant in the proceedings before the referring court, is a natural person on whom penalty points were imposed under the Law on motoring and a related decree. [11] The Ceļu satiksmes drošības direkcija (the Road Safety Directorate, Latvia, ‘the CSDD’) is a public body which entered those penalty points in the national vehicle register.

17. Since information relating to penalty points can be communicated upon request and was, according to B, transmitted for re-use to several companies, B filed a constitutional complaint with the referring court, challenging the conformity of Article 14^1 (2) of the Law on motoring with the right to privacy set out in Article 96 of the Latvijas Republikas Satversme (the Latvian Constitution).

18. Since Article 14^1 (2) of the Law on motoring was adopted by the Latvijas Republikas Saeima (Latvian Parliament, ‘the Saeima’), that institution participated in the proceedings. The CSDD, which processes the data at issue, was also heard. In addition, the Datu valsts inspekcija (Data Protection Authority, Latvia) – which in Latvia is the supervisory authority within the meaning of Article 51 of the GDPR – and several other authorities and persons were invited to give their opinion as *amici curiae* before the referring court.

10 In the amended version that entered into force on 10 May 2018.

11 Ministru kabineta 2004. gada 21. jūnija noteikumi Nr.551 “Pārkāpumu uzskaites punktu sistēmas piemērošanas noteikumi” (Cabinet Regulation Nr. 551, of 21 June 2004, “Rules for the application of penalty points system”).

19. The Saeima acknowledges that, under the provision at issue, any person may obtain information about another person's penalty points either by enquiring directly at the CSDD or by using the services provided by commercial re-users.

20. That being the case, the Saeima considers that the provision at issue is lawful because it is justified by the objective of improving road safety, which requires that traffic offenders be openly identified and that drivers be deterred from committing offences.

21. In addition, the right of access to information, provided for in Article 100 of the Latvian Constitution, should be respected. In any event, the processing of information relating to penalty points takes place under the control of the public authority and in compliance with appropriate safeguards for the rights and freedoms of data subjects.

22. The Saeima further explains that, in practice, communication of the information contained in the national vehicle register is subject to the condition that the person requesting the information provide the national identification number of the driver about whom he or she wishes to enquire. This precondition for obtaining information is explained by the fact that, unlike a person's name, a national identification number is a unique identifier.

23. The CSDD, for its part, explained to the referring court the functioning of the penalty points system and confirmed that the national legislation does not impose any limits on public access to and re-use of data relating to penalty points.

24. The CSDD also provided details of the contracts concluded with commercial re-users. It pointed out that these contracts do not provide for the legal transfer of data and that re-users ensure that the information transmitted to their customers does not exceed that which can be obtained from the CSDD. In addition, one of the contractual terms stipulates that the acquirer of the information must use it in the manner laid down in the regulations in force and in accordance with the purposes indicated in the contract.

25. The Data Protection Authority expressed doubts as to the compliance of the provision at issue with Article 96 of the Latvian Constitution. It did not rule out the possibility that the processing of the data at issue may be inappropriate or disproportionate.

26. That authority also observed that, although the statistics on traffic accidents in Latvia show a decrease in the number of accidents, there is no evidence that the penalty points system and public access to information relating to it have contributed to this favourable development.

27. The Satversmes tiesa (Constitutional Court) notes, first of all, that the proceedings before it do not concern Article 14^{1} (2) of the Law on motoring in its entirety, but only in so far as that provision makes information relating to penalty points entered in the national vehicle register accessible to the public.

28. That court further considers that penalty points are personal data and must therefore be processed in accordance with the right to respect for private life. It emphasises that in assessing the scope of Article 96 of the Latvian Constitution, account must be taken of the GDPR as well as of Article 16 TFEU and Article 8 of the Charter of Fundamental Rights of the European Union ('the Charter').

29. With regard to the objectives of the Law on motoring, the referring court states that it is with the aim of influencing the conduct of vehicle drivers and thus minimising the risks to life, health and property of persons, that offences committed by drivers, which are classified as administrative offences in Latvia, are entered in the national register of convictions and that penalty points are entered in the national vehicle register.

30. The national register of convictions constitutes a single register of convictions of persons who have committed offences (whether criminal or administrative), with the aim of, inter alia, facilitating the review of the penalties imposed. By contrast, the national vehicle register makes it possible to keep track of road traffic offences and to implement measures depending on the number of such offences committed. The penalty points system aims to improve road safety by distinguishing vehicle drivers who, systematically and in bad faith, disregard road traffic rules from drivers who occasionally commit offences, and by influencing the conduct of road users in a deterrent manner.

31. The referring court observes that Article 14^1 (2) of the Law on motoring gives any person the right to request and obtain from the CSDD the information in the national vehicle register relating to the penalty points imposed on drivers. In practice, information on penalty points is provided to the person requesting it as soon as the person indicates the national identification number of the driver concerned.

32. The Satversmes tiesa (Constitutional Court) subsequently clarifies that penalty points, by virtue of their classification as publicly available information, fall within the scope of the Law on the disclosure of information and may therefore be re-used for commercial or non-commercial purposes other than the original purpose for which the information was created.

33. In order to interpret and apply Article 96 of the Latvian Constitution in conformity with EU law, the referring court wishes to know, first, whether penalty points such as those imposed under Latvian law, fall within the scope of Article 10 of the GDPR. In particular, the referring court seeks to ascertain whether Article 14^1 (2) of the Law on motoring infringes the requirements contained in Article 10 of the GDPR that the processing of the data referred to in that provision may be carried out only 'under the control of official authority' or under 'appropriate safeguards for the rights and freedoms of data subjects'.

34. That court observes that Article 8(5) of Directive 95/46, which left it to each Member State to assess whether the special rules on data relating to offences and criminal convictions should be extended to data relating to administrative offences and penalties, was implemented in Latvia by Article 12 of the Fizisko personu datu aizsardzības likums (Law on the protection of data of natural persons), according to which personal data relating to administrative offences could, like data relating to criminal offences and convictions, be processed only by the persons, and in the circumstances, provided for by law.

35. It follows from this that for more than a decade similar requirements have been applied in Latvia for the processing of personal data relating to criminal offences and convictions and of personal data relating to administrative offences.

36. That court also observes that the scope of Article 10 of the GDPR must, in accordance with recital 4 of that regulation, be assessed taking into account the function of fundamental rights in society. It considers, in this respect, that the objective of ensuring that a person's private and professional life is not unduly adversely affected as a result of a previous conviction could apply both to criminal convictions and to administrative offences.

37. The Satversmes tiesa (Constitutional Court) seeks to ascertain, secondly, the scope of Article 5 of the GDPR. In particular, it wonders whether, in the light of recital 39 of that regulation, the Latvian legislature has complied with the obligation, set out in Article 5(1)(f) of the GDPR, to ensure that personal data are processed with 'integrity and confidentiality'. It observes that Article 14^1 (2) of the Law on motoring, which, by allowing access to information on penalty points, makes it possible to determine whether a person has been convicted of a road traffic offence, has not been accompanied by specific measures ensuring the security of such data.

38. The referring court wishes to know, thirdly, whether Directive 2003/98 is relevant to the assessment of whether Article 14^1 (2) of the Law on motoring is compatible with Article 96 of the Latvian Constitution. It points out that, pursuant to that directive, the re-use of personal data may be permitted only if the right to privacy is respected.

39. Fourthly, in the light of the Court's case-law according to which the interpretation of EU law provided in preliminary rulings has *erga omnes* and *ex tunc* effects, the referring court wonders whether it could nevertheless, if Article 14^1 (2) of the Law on motoring is found to be incompatible with Article 96 of the Latvian Constitution, read in the light of EU law as interpreted by the Court, rule that the legal effects of Article 14^1 (2) will be maintained until the date of delivery of its judgment in which it declares that that provision is unconstitutional, on the basis that a large number of legal relationships will be affected by its judgment.

40. In this respect, the referring court explains that, pursuant to Latvian law, an act which is declared unconstitutional is to be considered void from the day of publication of the Satversmes tiesa's (Constitutional Court) judgment, unless that court decides otherwise. It also explains its practice of seeking to strike a balance between the principle of legal certainty and the fundamental rights of the various parties concerned when determining the date from which the provision declared unconstitutional will no longer be in force.

41. It is against this background that, by order of 4 June 2019, received at the Court on 11 June 2019, the Satversmes tiesa (Constitutional Court) referred the following questions for a preliminary ruling:

'(1) Must the expression "processing of personal data relating to criminal convictions and offences or related security measures", used in Article 10 of the GDPR, be interpreted as meaning that it includes the processing of information relating to penalty points recorded against drivers for motoring offences as provided for in the provision at issue?

(2) Irrespective of the answer to the first question, can the provisions of the GDPR, in particular the principle of "integrity and confidentiality" referred to in Article 5(1)(f) thereof, be interpreted as meaning that they prohibit Member States from stipulating that information relating to penalty points recorded against drivers for motoring offences falls within the public domain and from allowing such data to be processed by being communicated?

(3) Must recitals 50 and 154, Article 5(1)(b) and Article 10 of the GDPR and Article 1(2)(cc) of Directive 2003/98 be interpreted as meaning that they preclude the legislation of a Member State which allows information relating to penalty points recorded against drivers for motoring offences to be transmitted for the purposes of re-use?

(4) If any of the foregoing questions is answered in the affirmative, must the principle of the primacy of EU law and the principle of legal certainty be interpreted as meaning that it might be permissible to apply the provision at issue and maintain its legal effects until such time as the decision ultimately adopted by the Satversmes tiesa (Constitutional Court) becomes final?'

42. Written observations were submitted by the Latvian, Dutch, Austrian and Portuguese Governments and by the European Commission.

43. Against the background of the spread of the SARS-CoV-2 virus, the Court decided to vacate the hearing of this matter which had been listed for 11 May 2020. By way of measures of organisation of procedure and as an exceptional step, the Court decided to replace that hearing with questions to be answered in writing. The Latvian and Swedish Governments and the Commission answered the questions put to them by the Court.

IV. Assessment

44. This request for a preliminary ruling raises a number of fundamental questions about the GDPR. All of these questions, however, presuppose the applicability of the GDPR to the case at issue.[12] I raise this point given the fact that the European Union has not legislated in the area of penalty points for driving offences.

A. On the material scope of the GDPR – Article 2(2)(a)

45. Pursuant to Article 2(2)(a) of the GDPR, that regulation does not apply to the processing of personal data in the course of an activity which falls outside the scope of EU law. It is apparent that while Article 2(1) of the GDPR positively formulates what falls under that regulation,[13] Article 2(2) excludes four types of activity from its scope. As an exception to the general rule, Article 2(2) of the GDPR must be interpreted strictly.[14]

46. The EU legislature has chosen to use a regulation as the form of legal instrument in order to increase the degree of uniformity of EU data protection law, in particular in order to create a level playing field among (economic) operators within the internal market, regardless of where those operators are based.[15]

47. Article 16 TFEU not only contains the legal basis for the adoption of texts such as the GDPR, but also constitutes, more generally, forming part of Part One, Title II, of the FEU Treaty,[16] a horizontal provision of a constitutional character which must be taken into account in the exercise of any EU competence.

48. Just as its predecessor, Directive 95/46, did, the GDPR seeks to ensure a high level of protection of the fundamental rights and freedoms of natural persons, in particular the right to privacy, with respect to the processing of personal data.[17]

12 Counter-intuitive as though this may appear, the wording 'scope of Union law', contained in Article 2(2)(a) of the GDPR, is all but clear in the context of the GDPR, see Wolff, H.A., in M. Pechstein, C. Nowak, U. Häde (eds), *Frankfurter Kommentar zu EUV, GRC und AEUV*, Band II, Mohr Siebeck, Tübingen, 2017, Art 16 AEUV, point 19.

13 Namely the processing of personal data wholly or partly by automated means and the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

14 With respect to Article 3(2) of Directive 95/46, the Court has consistently held as much, see judgment of 10 July 2018, *Jehovan todistajat* (C-25/17, EU:C:2018:551, paragraph 37 and the case-law cited). See also Sobotta, Chr., in E. Grabitz, M. Hilf and M. Nettesheim, *Das Recht der Europäischen Union*, 71. EL., updated August 2020, C.H. Beck, Munich, Art. 16 AEUV, point 22, who points to the wide scope *ratione materiae* of the EU data protection regime.

15 See also, in this respect, Hatje, A., in J. Schwarze, U. Becker, A. Hatje, J. Schoo (eds), *EU-Kommentar*, 4th ed., Nomos, Baden-Baden, 2019, Art. 16, point 10, and Brühann, U., in H. von der Groeben, J. Schwarze, A. Hatje (eds), *Europäisches Unionsrecht (Kommentar)*, *Band 1*, 7th ed., Nomos, Baden-Baden, 2015, Art. 16 AEUV, point 130.

16 On 'provisions having general application'.

17 See, with respect to Directive 95/46, by way of example, judgments of 13 May 2014, *Google Spain and Google* (C-131/12, EU:C:2014:317, paragraph 66), and of 10 July 2018, *Jehovan todistajat* (C-25/17, EU:C:2018:551, paragraph 35).

49. The wording of Article 2(2)(a) of the GDPR essentially mirrors that of Article 16(2) TFEU,[18] which constitutes the legal basis of that regulation under primary law. According to Article 16(2) TFEU, the EU legislature is to lay down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States 'when carrying out *activities which fall within the scope of Union law*, and the rules relating to the free movement of such data'.[19] That provision is, therefore, declaratory in nature. Accordingly, the analysis which follows applies to Article 2(2)(a) of the GDPR and Article 16(2) TFEU in equal measure.

50. The first thing to note is that the wording of Article 2(2)(a) of the GDPR ('an activity which falls outside the scope of Union law') differs from that of Article 51(1) of the Charter,[20] according to which 'the provisions of the Charter are addressed to … the Member States *only when they are implementing Union law*'.[21]

51. If one were to see this as an indication that the wording of Article 2(2)(a) of the GDPR is wider than that of Article 51(1) of the Charter,[22] given that the Court has interpreted Article 51(1) of the Charter to mean that the Charter applies 'where national legislation falls within the scope of European Union law',[23] there is no substantial difference between the wording of these two provisions as interpreted by the Court.[24]

52. That said, I do not think that analogies with the Court's case-law on the field of application of the Charter should be drawn.[25] That would be too restrictive and would be counter to the objective pursued by Article 16 TFEU and by the GDPR. Indeed, the logic of the Charter is wholly different from that of the GDPR: the Charter seeks to domesticate the exercise of power by the EU institutions and Member States when they operate within the scope of EU law and, conversely, provide a shield for individuals to assert their respective rights. By contrast, the protection of personal data is more than a fundamental right. As is demonstrated by Article 16 TFEU,[26] data protection constitutes an EU policy field in its own right. The very purpose of the GDPR is that it is to apply to *any* form of processing of personal data, regardless of the subject matter involved – and this, incidentally, whether carried out by Member States or individuals. Interpreting the terms of Article 2(2)(a) of the GDPR restrictively would completely frustrate that objective. The GDPR, which was intended to be a tiger for data protection, would turn out to be a domestic kitten.

18 The initial internal market-related rationale of the EU regulating the data protection regime continues to persist next to the protection of data in its own right. As is reflected already in its title and defined in its Article 1, the GDPR's subject matter and objective is twofold: to lay down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. Moreover, recital 13 of the GDPR specifies that divergences hampering the free movement of personal data within the internal market are to be prevented and that the proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

19 My emphasis.

20 This provision defines the field of application of the Charter.

21 My emphasis.

22 See, for instance, Zerdick, Th., in E. Ehmann, M. Selmayr (eds), *Datenschutz-Grundverordnung, Kommentar*, C.H. Beck, Munich, 2nd ed., 2018, Art. 2, point 5.

23 This constitutes consistent case-law since judgment of 26 February 2013, *Åkerberg Fransson* (C-617/10, EU:C:2013:105, paragraph 21). See also judgments of 21 December 2016, *AGET Iraklis* (C-201/15, EU:C:2016:972, paragraph 62); of 21 May 2019, *Commission* v *Hungary (Usufruct over agricultural land)* (C-235/17, EU:C:2019:432, paragraph 63); and of 24 September 2020, *NK (Pensions d'entreprise de personnel cadre)* (C-223/19, EU:C:2020:753, paragraph 78).

24 The wording of Article 2(2)(a) of the GDPR is, I would submit, inconclusive. In accordance with the settled case-law of the Court, in interpreting a provision of EU law, it is necessary to consider not only its wording but also its context and the objectives of the legislation of which it forms part, and in particular the origin of that legislation, see, by way of example, judgment of 17 April 2018, *Egenberger* (C-414/16, EU:C:2018:257, paragraph 44 and the case-law cited).

25 See in this sense also Lubasz, D., in D. Lubasz (ed.), *Ochrona danych osobowych*, Wolters Kluwer, Warsaw 2020, point 92.

26 And was formerly equally true of Article 114 TFEU.

53. The mere existence of a provision such as Article 10 of the GDPR, which will be interpreted in detail below in my analysis of the referring court's first question, is a case in point in this respect. If the GDPR deals with 'processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1)' of the GDPR,[27] at a time when criminal convictions and offences are almost exclusively determined under national and not EU law, short of Article 10 of the GDPR being invalid, that regulation cannot have the accessory function which is proper to the Charter.

54. The same applies to the existence of Article 87 of the GDPR, which allows Member States to further determine the specific conditions for the processing of a national identification number.[28]

55. Moreover, account should be taken of recital 16 of the GDPR which, in the non-prescriptive but nevertheless instructive part of that regulation, mirrors Article 2 of the GDPR. Here, national security is mentioned as an example of an area falling outside the scope of EU law. The same goes for the equally non-binding declaration on Article 16 of the FEU Treaty[29] where it is declared that 'whenever rules on protection of personal data to be adopted on the basis of Article 16 [TFEU] could have direct implications for national security, due account will have to be taken of the specific characteristics of the matter' and where it is recalled that 'in particular Directive 95/46 … includes specific derogations in this regard'.[30]

56. This explicit focus on national security is a clear indication of what both the FEU Treaty authors (Article 16 TFEU) and the EU legislature (Article 2(2)a of the GDPR) had in mind when they drafted the respective passages.

57. The EU legislature has specified elsewhere, still in the context of data protection, that national security is in this context to be understood as 'State security'.[31]

58. In this connection, Article 2(2)(a) of the GDPR should be seen against the background of Article 4(2) TEU, which provides that the European Union is to respect Member States' essential State functions[32] and in this respect specifies, by way of example, that 'national security remains the sole responsibility of each Member State'. Article 2(2)(a) of the GDPR does nothing more than reiterate this constitutional requirement of what must be guaranteed for a State to function.[33]

59. On the basis of the preceding analysis, I have no grounds to believe that Article 2(2)(a) of the GDPR introduces a test with a high threshold to be met in order to trigger the applicability of the GDPR, nor that this would have been the intention of the EU legislature.

27 See Article 10 of the GDPR.

28 Particularly if one considers that a national identification number is usually given on the occasion of the official registration of a birth, a subject matter not typically associated with an EU competence.

29 See Declaration n° 20 annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, signed on 13 December 2007.

30 As a result of Article 94(2) of the GDPR, references to Directive 95/46 are to be construed as references to the GDPR.

31 See Article 15(1) of 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). See, on this provision, judgment of 29 January 2008, *Promusicae* (C-275/06, EU:C:2008:54, paragraph 49).

32 Including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security.

33 See, for this term, Franzius, C., in M. Pechstein, C. Nowak, U. Häde (eds), *Frankfurter Kommentar zu EUV, GRC und AEUV, Band I*, Mohr Siebeck, Tübingen, 2017, Art. 4 EUV, point 50: '*Staatsfunktionengarantie*'.

60. Finally, a quick glance at the remaining three exceptions to the material scope of the GDPR, contained in Article 2(2)(b) to (d), confirms this analysis. The GDPR thus does not apply to the processing of personal data by the Member States when carrying out activities within the scope of the EU's common foreign and security policy,[34] by a natural person in the course of a purely personal or household activity,[35] and 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.[36]

61. The exclusion of the common foreign and security policy, which remains predominantly intergovernmental, is only logical.[37] Purely personal and household activities of natural persons are in any event, in principle, outside the scope of EU law since they are not governed by primary or secondary law. The same applies, in principle, to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Nevertheless, the reason for this last exception is that the Union has adopted a specialised directive,[38] incidentally on the same date on which the GDPR was adopted. In addition, it is apparent from Article 23(1)(d) of the GDPR that the processing of personal data carried out by *individuals* for the same purposes falls within the scope of the GDPR.[39]

62. Accordingly, if they are to have any normative legal significance, the last two exceptions cannot be held to fall outside the scope of EU law *within the meaning of Article 2(2)(a) of the GDPR*.

63. Finally, it should be pointed out that there is no discernible evidence that the Court would, as a matter of principle, apply a strict test as to the scope of the GDPR or Directive 95/46 under Article 2 of the GDPR and Article 3 of Directive 95/46, respectively.[40] On the contrary, the Court tends to stress that 'the applicability of Directive 95/46 cannot depend on whether the specific situations at issue in the main proceedings have a sufficient link with the exercise of the fundamental freedoms guaranteed by the Treaty'.[41]

64. To conclude this preliminary part of the analysis, on a proper construction of Article 2(2)(a) of the GDPR, that regulation applies to the processing of personal data in or by a Member State, unless that processing is carried out in an area where the European Union does not have competence.

65. As a consequence, the GDPR is applicable to the case at issue and must be taken into account by the referring court in examining the validity of the national law.

B. On Article 86 of the GDPR

66. For the sake of completeness, I would like briefly to address the provision of Article 86 of the GDPR in the case at issue.

34 See Article 2(2)(b) of the GDPR.

35 See Article 2(2)(c) of the GDPR.

36 See Article 2(2)(d) of the GDPR.

37 Moreover, Article 39 TEU contains a specific legal basis for data processing of personal data by the Member States when carrying out activities under the common foreign and security policy. Ergo, 'pillar' distinction has been maintained in this respect with the Treaty of Lisbon, see Lynskey, O., *The Foundations of EU Data Protection Law*, OUP, Oxford, 2015, p. 18.

38 See Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89).

39 See, moreover, 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, paragraph 102).

40 To give just one example, the Court thus did not actively scrutinise whether charitable and religious activities fell within the scope of EU law (see judgment of 6 November 2003, *Lindqvist*, C-101/01, EU:C:2003:596, paragraph 48).

41 See judgment of 20 May 2003, *Österreichischer Rundfunk and Others* (C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 42).

67. Pursuant to that article, personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with EU or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to the GDPR.

68. All that provision does is acknowledge the importance of public access to official documents. Moreover, as the Commission has rightly pointed out, no further guidance is given in that provision on how public access to official documents should be reconciled with data protection rules.[42] The provision is rather declaratory in nature, which is more akin to a recital than a prescriptive provision of a legal text.[43] As a consequence, I would submit that the 'narrative norm' of Article 86 of the GDPR does not have any bearing on the analysis that follows.

C. First Question: Penalty points under Article 10 of the GDPR

69. By its first question, the referring court seeks to ascertain whether Article 10 of the GDPR is to be interpreted as meaning that it covers situations of processing of information relating to penalty points recorded against drivers for motoring offences as provided for by national law.

70. Pursuant to that provision, processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) of the GDPR[44] is to be carried out only under the control of official authority.[45] Any comprehensive register of criminal convictions is to be kept only under the control of official authority.

71. In view of the fact that the CSDD appears to be an official – in the sense of 'public' – authority, one may question the pertinence of the first question and wonder whether it is hypothetical in the sense of the Court's case-law on admissibility. Nevertheless, I would dispel such doubts by pointing out that the present case concerns both the communication of penalty points (by the CSDD) and the re-use of that data by other bodies. To the extent that the first question refers to those other bodies, it is, in my view, admissible.

1. Personal data

72. Article 4(1) of the GDPR stipulates that 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data or online identifier or to one or more factors specific to the physical physiological, genetic, mental, economic cultural or social identity of that natural person.

73. There is no reason to doubt that information relating to penalty points recorded against drivers for motoring offences constitutes personal data within the meaning of Article 4(1) of the GDPR.

42 In legal doctrine, see moreover Kranenborg, H., in Chr. Kuner, L.A. Bygrave, Chr. Docksey (eds), *The EU General Data Protection Regulation (GDPR)*, OUP, Oxford, 2020, Art. 86, A., at p. 1214. See also Pauly, D.A., in B.P. Paal, D.A. Pauly, *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*, C.H. Beck, Munich 2018, Art. 86 DS-GVO, point 9.

43 See also, in that regard, Kranenborg, H., op. cit., Art. 86, C.1., at p. 1217, including footnote 14. The same author quite rightly points to the fact that, in the initial Commission proposal, only a recital and no provision on the matter was included.

44 According to this provision, if the data subject has given consent to the processing of his/her personal data for one or more specific purposes, processing is lawful to the extent of the consent given.

45 Or when the processing is authorised by EU law or a Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

2. … relating to criminal convictions and offences or related security measures

74. As regards the 'offences' mentioned in Article 10 of the GDPR, it should be noted that it is not entirely clear in all language versions of that provision whether it refers to *criminal* offences only or whether it also covers *administrative* offences. The most natural and intuitive interpretation of the English language version is that the term 'criminal' has been placed, so to speak, before the bracket and refers to both 'convictions' and 'offences'. In this connection, some language versions [46] do not leave any room for doubt: 'offences' within the meaning of Article 10 of the GDPR are to be construed as 'criminal'. Other language versions [47] are ambiguous in that they are open to more than one interpretation. The Latvian language version (*saistītiem drošības pasākumiem*), which, it is to be presumed, is the language version the referring court is most familiar with, is also ambiguous. Here, not only is it not specified whether 'offences' (*pārkāpumi*) are to be criminal in nature, but it is also left open whether 'convictions' (*sodāmība*) are to be criminal in nature. [48]

75. Even if the different language versions may appear variegated, some conclusions can nevertheless be drawn at this point.

76. All the official languages of the European Union are the authentic languages of the acts in which they are drafted and, therefore, all the language versions of an act of the European Union must, as a matter of principle, be recognised as having the same value. [49] An interpretation of a provision of EU law thus involves a comparison of the different language versions. [50] Moreover, the various language versions of a text of EU law must be given a uniform interpretation. [51]

77. In those circumstances, it is the meaning of the more 'precise' language versions which must be taken to be correct, in particular since this more precise meaning is also one of the possible interpretations under the less precise language versions, where one possibility is that 'offences' are interpreted as only 'criminal' in nature. I can therefore provisionally conclude at this stage that, on the basis of a comparative reading of the different language versions of Article 10 of the GDPR, the term 'criminal' refers both to 'convictions' and 'offences'. [52]

78. Moreover, that proposed interpretation of Article 10 of the GDPR retains the distinction made in its precursor, Article 8(5) of Directive 95/46. Under that previous provision, the control of official authority was required for the processing of data relating to criminal convictions and offences, [53] whereas for administrative sanctions there was the possibility of making the processing of data subject to the control of official authority. [54] If under Article 8(5) of Directive 95/46 the term 'offences' had been understood to encompass 'administrative offences', then the second limb of that provision would have been redundant.

46 Such as the Spanish (*condenas e infracciones penales*), German (*strafrechtliche Verurteilungen und Straftaten*), Italian *condanne penali e […] reati*), Lithuanian (*apkaltinamuosius nuosprendžius ir nusikalstamas veikas*), Maltese (*kundanni kriminali u reati*) and Dutch (*strafrechtelijke veroordelingen en strafbare feiten*) language versions.

47 Such as the French (*condamnations pénales et […] infractions*), Polish (*wyroków skazujących oraz naruszeń prawa*), Portuguese (*condenações penais e infrações*) and Romanian (*condamnări penale și infracțiuni*) language versions.

48 In fact, on a pure reading of the wording, even 'convictions' could theoretically be administrative in nature.

49 See, by way of example, judgment of 25 June 2020, *A and Others (Wind turbines at Aalter and Nevele)* (C-24/19, EU:C:2020:503, paragraph 39 and the case-law cited).

50 See judgment of 6 October 1982, *Cilfit and Others* (283/81, EU:C:1982:335, paragraph 18).

51 See, by way of example, judgments of 30 May 2013, *Genil 48 and Comercial Hostelera de Grandes Vinos* (C-604/11, EU:C:2013:344, paragraph 38 and the case-law cited), and of 6 September 2012, *Parliament* v *Council* (C-490/10, EU:C:2012:525, paragraph 68).

52 See in this sense also Kawecki, M., Barta, P, in P. Litwiński (ed.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, C.H. Beck, Warsaw 2018, Art. 10, point 3.

53 'Processing of data relating to offences, criminal convictions or security measures *may be carried out only* under the control of official authority …'. My emphasis.

54 'Member States *may* provide that data relating to administrative sanctions or judgments in civil cases shall also be processed under the control of judicial authority'. My emphasis.

79. This finding still leaves open the question of what exactly is to be understood by the term 'criminal offences'.

80. The first issue here is whether that term constitutes an autonomous term of EU law or whether the interpretation of the term is left to the Member States.

81. According to settled case-law of the Court, the need for a uniform application of EU law and the principle of equality require that the wording of a provision of EU law which makes no express reference to the law of the Member States for the purpose of determining its meaning and scope must normally be given an autonomous and uniform interpretation throughout the European Union.[55] That interpretation must take into account the wording, objectives and legislative context of the provision in question as well as the provisions of EU law as a whole. The origins of a provision of EU law may also provide information relevant to its interpretation.[56]

82. Here, it is clear that, in principle, criminal legislation and rules of criminal procedure are matters for which the Member States are responsible.[57] As a consequence, Member States will be in a position to determine what constitutes an offence.[58]

83. However, once the EU legislature has chosen the legal form of a regulation, as opposed to a directive, I would submit that a uniform interpretation throughout the European Union of the terms of that regulation should be the norm, so as to ensure its general application and direct applicability in all Member States, in line with Article 288(2) TFEU.

84. In a similar vein, there are indications that the Union legislature did not wish to refer to national law(s) as regards the interpretation of the term 'offences'. Thus, recital 13 of Directive 2016/680[59] states that a criminal offence within the meaning of that directive should be an autonomous concept of EU law as interpreted by the Court of Justice of the European Union. In a spirit of *a maiore ad minus*, I would submit that such a statement also applies to the GDPR which, as stated above, constitutes, as a regulation, a legal act which automatically possesses a higher degree of integration and centralisation.

85. The second issue, which consists in establishing whether the personal data in question relates to criminal convictions and offences or related security measures within the meaning of Article 10 of the GDPR, is more difficult.

86. The Court has previously had occasion to rule on the definition of a 'criminal offence' in the context of the *ne bis in idem* principle[60] under Article 50 of the Charter.[61]

87. Here, the Court draws on case-law of the European Court of Human Rights,[62] according to which three criteria are relevant in defining the term 'criminal proceedings': the legal classification of the offence under national law, the very nature of the offence, and the nature and degree of severity of the penalty that the person concerned is liable to incur.[63]

55 See, by way of example, judgment of 1 October 2019, *Planet49* (C-673/17, EU:C:2019:801, paragraph 47 and the case-law cited).

56 Ibid.

57 See judgment of 17 September 2020, *JZ (Custodial sentence in the case of an entry ban)* (C-806/18, EU:C:2020:724, paragraph 26 and the case-law cited).

58 See also, in this sense, Georgieva, L., *The EU General Data Protection Regulation (GDPR)*, op. cit., Art. 10, C.1., at p. 388, and Schiff, A., *Datenschutz-Grundverordnung, Kommentar*, op. cit., Art. 10, point 4.

59 Which, incidentally, was adopted on the same day as the GDPR.

60 The right not to be tried or punished twice in criminal proceedings for the same criminal offence.

61 See also the instructive Opinion of Advocate General Kokott in *Bonda* (C-489/10, EU:C:2011:845, point 32 *et seq.*).

62 See judgment of the Court of Human Rights of 8 June 1976, *Engel and Others v. the Netherlands* (CE:ECHR:1976:0608JUD000510071, §§ 80 to 82), and of 10 February 2009, *Sergey Zolotukhin v. Russia* (CE:ECHR:2009:0210JUD001493903, §§ 52 and 53).

63 See judgment of 5 June 2012, *Bonda* (C-489/10, EU:C:2012:319, paragraph 37).

88. Penalty points such as those imposed under the national law in question do not, in my view, qualify as a criminal offence under that case-law as they do not fulfil those criteria. In particular, they are not very severe in nature. [64]

89. Finally, I should like to point out that, as a result of this analysis, there is no need to examine the delimitation between Article 10 of the GDPR and the provisions of Directive 2016/680, since that directive is not applicable to the case at issue.

3. Proposed reply

90. I therefore propose to answer the first question to the effect that Article 10 of the GDPR is to be interpreted as meaning that it does not cover situations of processing of information relating to penalty points recorded against drivers for motoring offences as provided for by a national law such as Article 14^1 (2) of the Law on motoring.

D. Second Question: Communicating penalty points

91. By its second question, the referring court seeks to ascertain, in essence, whether the provisions of the GDPR preclude a Member State from processing and communicating information relating to penalty points recorded against drivers for motoring offences.

92. Although the referring court points, by way of example, to the principle of integrity and confidentiality contained in Article 5(1)(f) of the GDPR, [65] the question is worded in broad terms, since it refers to the provisions of that regulation as a whole. [66] The analysis below will therefore extend to provisions of the GDPR other than that mentioned by the referring court in its question.

93. All processing of personal data must comply, first, with the principles relating to data quality set out in Article 5 of the GDPR and, second, with one of the criteria governing the legitimacy of data processing listed in Article 6 of that regulation. [67] We can infer from the wording of those two provisions that the former are cumulative [68] and the latter alternative in nature. [69]

94. The second question relates to the data quality principles. The referring court appears – quite rightly – to assume that the CSDD processes data and it does not question the recording of the penalty points as such, but the communication of the points on request.

95. The CSDD is undeniably a 'controller' within the meaning of Article 4, point 7, of the GDPR, which processes personal data within the meaning of Article 4, point 2, of that regulation by recording the penalty points in the national vehicle register.

64 Given that we are dealing here with penalty points which are, as seen, not severe in nature, this finding is not called into question by the Court's ruling in its judgment of 14 November, *Baláž* (C-60/12, EU:C:2013:733), which dealt with the wider and more general issue of 'jurisdiction in particular in criminal matters' as regards road traffic offences in general and not only with regard to penalty points in the context of Council Framework Decision 2005/214/JHA of 24 February 2005 on the application of the principle of mutual recognition to financial penalties (OJ 2005 L 76, p. 16).

65 Which, as will be seen below, is not applicable in any event.

66 Against this background one could legitimately question whether the requirements of Article 94, lit c., of the Rules of Procedure of the Court are complied with, failing which, the question would be inadmissible.

67 See judgment of 16 January 2019, *Deutsche Post* (C-496/17, EU:C:2019:26, paragraph 57 and the case-law cited).

68 Article 5 of the GDPR is formulated in a prescriptive manner ('shall') and the various principles are linked by semicolons, implying an 'and' and not an 'or'.

69 Article 6 of the GDPR refers to 'at least one of the … principles'.

96. Suffice it to point out that the Court has held, with respect to a publicly held 'companies register', that by transcribing and keeping information in that register and communicating it, where appropriate, on request to third parties, the authority responsible for maintaining that register carries out 'processing of personal data' for which it is the 'controller', within the meaning of those definitions set out in Directive 95/46,[70] which constitute the precursors to the definitions set out in Article 4, points 2 and 7, of the GDPR.[71]

1. On Article 5(1)(f) of the GDPR: Integrity and confidentiality

97. This raises the question whether the principles of integrity and confidentiality set out in Article 5(1)(f) of the GDPR – a provision to which the referring court itself refers in its question – have been respected.

98. Pursuant to Article 5(1)(f) of the GDPR, personal data is to be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

99. As is clear from its wording, this provision concerns *security*, *technical* and *organisational* measures used in connection with the processing of personal data.[72] We are dealing here with general formal requirements regarding security of data.[73]

100. By contrast, the referring court is seeking guidance which is more fundamental and which relates to the *legal possibility* of such processing. Put differently and in more figurative terms, it seeks guidance on the *if* of the processing of personal data, whereas Article 5(1)(f) of the GDPR deals with the *how* of such processing. As a consequence, Article 5(1)(f) of the GDPR is not of relevance for the case at issue.

2. On Article 5(1)(a) of the GDPR: Lawfulness, fairness and transparency

101. Pursuant to Article 5(1)(a) of the GDPR, personal data is to be processed lawfully, fairly and in a transparent manner in relation to the data subject.

102. It should be noted that the term 'lawfulness' appears both in Article 5(1)(a) and in Article 6 of the GDPR. Reading the detailed requirements of Article 6 into Article 5 of that regulation would make little sense from the perspective of legislative drafting if Article 5 were also to contain the criteria of Article 6 of the GDPR.

70 See judgment of 9 March 2017, *Manni* (C-398/15, EU:C:2017:197, paragraph 35).

71 Articles 2(b) and (d) of Directive 95/46.

72 This principle is further developed in Chapter IV, Section 2, of the GDPR (Articles 32 to 34).

73 See also, to that effect, Pötters, St., in P. Gola (ed.), *Datenschutz-Grundverordnung VO (EU) 2016/679, Kommentar*, C.H. Beck, Munich, 2nd ed., 2018, Art. 5, point 29.

103. Instead, lawfulness within the meaning of Article 5(1)(a) of the GDPR should be read in the light of recital 40 of that regulation,[74] which requires processing to be based on either consent or another legal basis, laid down by law.[75]

104. That being so (there is a legal basis under national law), I see no reason to question the lawfulness of the processing in the case at issue.[76]

105. I therefore agree with the submissions of the Austrian Government[77] that this principle is not relevant to the facts of the case at issue.

3. On Article 5(1)(b) of the GDPR: Purpose limitation

106. Article 5(1)(b) of the GDPR lays down the principle of 'purpose limitation' by stating that personal data is to be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.[78]

107. The referring court explains that the provision at issue, Article 14^1 (2) of the Law on motoring, pursues the aim of road safety by exposing drivers who are in contravention of the rules. As such, communication of the penalty points appears to be a specified, explicit and legitimate purpose. Moreover, the processing of personal data does not appear incompatible with that purpose.

4. On Article 5(1)(c) of the GDPR: Data minimisation

108. Pursuant to Article 5(1)(c) of the GDPR, the principle of data minimisation requires personal data to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. Correspondingly, recital 39 of the GDPR states that personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

109. As with the other principles enshrined in Article 5(1) of the GDPR, I understand this principle to reflect the principle of proportionality,[79] which is why I consider it appropriate to examine at this stage whether the national law in question is proportionate to the objective it seeks to achieve.

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

75 See also, in that regard, Herbst, T., in J. Buchner, B. Kühling (eds), *Datenschutz-Grundverordnung/BDSG, Kommentar*, 2nd ed., C.H. Beck, Munich, 2018, Art. 5 DS-GVO, point 11, and Pötters, St., op. cit., Art. 5, point 6. For a broader understanding of lawfulness as requiring compliance with all provisions of the regulation, see Lubasz, D., in D. Lubasz (ed.), *Ochrona danych osobowych*, Wolters Kluwer, Warsaw 2020, point 186.

76 And even if one considers it necessary to check the requirements of Article 6 of the GDPR within Article 5 of that regulation, I would also consider the processing to be lawful within the meaning of Article 6(1)(c) of the GDPR, as processing that is necessary for compliance with a legal obligation to which the controller is subject, given that the CSDD, by communicating the penalty points to the public, fulfils its legal obligation under national law.

77 As regards the Austrian Government's reference in this connection to the judgment of the Bundesverfassungsgericht (Federal Constitutional Court) of 27 February 2008 (1 BvR 370/07 and 1 BvR 595/07 (ECLI:DE:BVerfG:2008:rs20080227.1bvr037007), BVerfGE 120, 274 et seq., at p. 314, available at: http://www.bverfg.de/e/rs20080227_1bvr037007en.html), I am less sure of its pertinence given that that judgment concerns a material fundamental right, whereas Article 5(1)(f) of the GDPR is, as established in the preceding paragraphs of this Opinion, about formal requirements.

78 The provision goes on to state that further processing for archiving purposes in the public interest, scientific or historical and research purposes or statistical purposes shall, in accordance with Article 89(1) of the GDPR, not be considered to be incompatible with the initial purposes.

79 See, to that effect, Lubasz, D., in D. Lubasz (ed.), *Ochrona danych osobowych*, Wolters Kluwer, Warsaw 2020, point 202.

110. It is settled case-law that the principle of proportionality, as a general principle of EU law, requires that measures implemented by acts of the European Union are appropriate for attaining the objective pursued and do not go beyond what is necessary to achieve it.[80]

111. Indeed, Article 14^1 (2) of the Law on motoring must be appropriate and necessary in order to pursue its purported aim, namely to enhance road safety.

(a) Appropriateness

112. The first purported objective of the national law at issue is to identify vehicle drivers who systematically disregard the rules of the road traffic system. It is clear that the identification of road traffic rule offenders does not depend in any way on the public nature (generally available) of the penalty points imposed on the perpetrator of an offence. It is the sole responsibility of a public authority accurately to identify such offenders and to keep records of the penalty points imposed on them so that the appropriate legal consequences follow and relevant sanctions can be applied.

113. The second objective of the national law provision authorising the disclosure of the personal data in question, invoked by the Saeima, is to influence the conduct of road users in order to discourage possible offenders from committing further offences. Here, it could be accepted that giving any person the opportunity to know who is breaking traffic rules is likely to have some deterrent effect: many drivers would object to such information about them being disclosed to the general public, so as not to be labelled as lawbreakers.

114. That aim is also clearly stated in Article 43^1 of the Law on motoring as the objective pursued by the introduction of the penalty points system. It is quite obvious that making penalty points public may, to a certain extent, constitute an additional deterrent factor. The provision at issue would thus, in principle, be in line with the general interest pursued, namely to promote road safety and avoid traffic accidents.

115. That said, if the personal data in question are made available only on request and if the applicant provides the personal identification number of the person concerned, this raises the question of how difficult it is to obtain that number. Indeed, the more difficult it is to obtain such data, the less dissuasive the disclosure regime will be, since whether that data are publicly available will depend on other factors that are difficult to predict.

116. It is for that reason that I have grave doubts as to the appropriateness of the national law in question.

117. It is for the referring court to decide, in the light of all the circumstances of the case, whether Article 14^1 (2) of the Law on motoring is genuinely appropriate for achieving the legitimate objective of improving road safety.

(b) Necessity

118. As regards the question of necessity, that it to say, the requirement that the measure in question must not go beyond what is necessary to achieve the objective pursued, the situation appears more clear-cut.

80 See, by way of example, judgment of 9 November 2010, *Volker und Markus Schecke and Eifert* (C-92/09 and C-93/09, EU:C:2010:662, paragraph 74 and the case-law cited).

119. Again, it is for the referring court to decide, in the light of all the circumstances of the case, whether the provision at issue is genuinely necessary. However, on the basis of the information available, I do not see how that provision could on any view be regarded as necessary.

120. Although the objective of promoting road safety is important, it is necessary to strike a fair balance between the different interests involved and, consequently, it is for the national legislature to decide whether the disclosure of the personal data in question goes beyond what is necessary to achieve the legitimate objectives pursued, having regard in particular to the infringement of fundamental rights generated by such disclosure.

121. The order for reference does not indicate whether the Saeima, prior to the adoption of the provision at issue, considered other means of achieving the objective of promoting road safety which would have led to less interference with the right of individuals to data protection. Furthermore, the legislature must be able to demonstrate that the derogations and limitations to data protection would be in strict compliance with the limits imposed. A careful assessment of the impact on data protection should be carried out before publishing a data set (or before adopting a law requiring its publication), including an assessment of the possibilities for re-use and the potential impact of re-use.

122. The existence and accuracy of such information is essential for deciding whether the objectives of fostering road safety and reducing traffic accidents can be achieved by measures which would be less detrimental to the rights of the persons concerned and thus avoid or at least mitigate a breach of the protection afforded by Article 8 of the Charter.

123. The invasion of privacy caused by the publication of data on offences and penalties imposed is, in itself, particularly serious: it discloses to the general public information about offences committed by an individual. Moreover, it cannot be excluded that such data processing inherent in the publication of the data in question may lead to the stigmatisation of the offender and other negative consequences. Therefore, such 'blacklists' must be strictly regulated.

124. Finally, as stated by the Data Protection Authority, the preventive nature of the provision at issue and the statistics indicating favourable trends, namely a reduction in the number of traffic accidents, do not show that that reduction is linked to the introduction of the penalty points system per se or to the fact that information relating to the penalty points recorded is publicly accessible.

5. Proposed reply

125. My proposal to the Court as to the reply to the second question is, accordingly, that a national law such as Article 14^1 (2) of the Law on motoring which allows for the processing and communicating of information relating to penalty points recorded against drivers for motoring offences is precluded by Article 5(1)(c) of the GDPR.

E. Third Question: Re-use of personal data

1. On Directive 2003/98

126. As set out in Article 1(1) of Directive 2003/98, that directive establishes a minimum set of rules governing the re-use and the practical means of facilitating re-use of existing documents held by public sector bodies of the Member States.

127. We can assume, for present purposes, that penalty points in Latvia are recorded in documents held by the CSDD as a public sector body within the meaning of that provision.

128. However, we are not within the scope of Directive 2003/98, given that Article 1(2)(cc) thereof states that that directive is not to apply to documents access to which is excluded or restricted by virtue of the access regimes on the grounds of protection of personal data.[81] Moreover, by virtue of Article 1(4) of Directive 2003/98, that directive leaves intact and in no way affects the level of protection of individuals with regard to the processing of personal data under the provisions of EU and national law, and in particular does not alter the obligations and rights set out in the GDPR.[82]

129. It follows from those provisions that the processing of the personal data in question must be assessed in the light of EU rules on data protection, namely the GDPR, and not Directive 2003/98.[83]

2. On re-use

130. As the referring court rightly notes, if information relating to penalty points recorded against drivers for motoring offences can be communicated to anyone, including re-use operators, it will not be possible to identify the purposes of the further processing of the data or to evaluate whether personal data are being processed in a manner that is incompatible with those purposes.

131. Against that background, my analysis of the second question referred fully applies not only *mutatis mutandis* but also a fortiori: private companies might be tempted to exploit personal data for commercial purposes, that is to say, for purposes that are incompatible with the purpose of the processing, which is to increase road safety.

132. Moreover, the possibility of third parties being able to process the personal data clearly goes beyond the purpose limitation established by Article 5(1)(b) of the GDPR.

3. Proposed reply

133. Accordingly, I propose to reply to the third question to the effect that a national law such as Article 14^1 (2) of the Law on motoring, which allows for the processing and communicating, including for the purposes of re-use, of information relating to penalty points recorded against drivers for motoring offences, is not governed by the provisions of Directive 2003/98. It is, moreover, precluded by Article 5(1)(c) of the GDPR.

F. Fourth Question

134. By its fourth question, the referring court seeks to ascertain whether – if it is established that the national law in question is contrary to EU law – it would be possible to apply the provision at issue and maintain its legal effects until such time as the decision ultimately adopted by the Satversmes tiesa (Constitutional Court) becomes final.

135. The referring court therefore requests that the legal effects of the provision at issue be maintained until it has given a final ruling.

81 This provision was added to Directive 2003/98 in 2013, see Article 1(1)(a)(iii) of Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information (OJ 2013 L 175, pp. 1 to 8).

82 Article 1(4) of Directive 2003/98 in this respect refers to Directive 95/46.

83 As for Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (OJ 2019 L 172, p. 56), which, by virtue of its Article 19, repeals Directive 2003/98 with effect from 17 July 2021, see Article 1(2)(f) of Directive 2019/1024.

136. According to settled case-law, the interpretation which, in the exercise of the jurisdiction conferred on it by Article 267 TFEU, the Court gives to a rule of EU law clarifies and defines the meaning and scope of that rule as it must be or ought to have been understood and applied from the date of its entry into force.[84] It follows that the rule as thus interpreted may, and must, be applied by the courts to legal relationships which arose and were established before the judgment ruling on the request for interpretation, provided that in other respects the conditions for bringing a dispute relating to the application of that rule before the courts having jurisdiction are satisfied.[85] It is only quite exceptionally that the Court itself may, in application of the general principle of legal certainty inherent in the EU legal order, be moved to restrict for any person concerned the opportunity of relying on a provision which it has interpreted with a view to calling into question legal relationships established in good faith.[86]

137. In any event, it is solely the Court which could determine the conditions of a possible suspension[87] and this for a good reason: otherwise, a national court could defer the effects of that decision, thereby affecting its *erga omnes* character, the primary objective of which is to ensure the uniform application of EU law and legal certainty in all Member States and create a level playing-field for Member States, citizens and economic operators. In this connection, rules of national law, even of a constitutional order, cannot be allowed to undermine the unity and effectiveness of EU law.[88]

138. Two essential criteria must be fulfilled before such a limitation can be imposed, namely that those concerned should have acted in good faith and that there should be a risk of serious difficulties.[89]

139. It should be added that it is only exceptionally[90] that the Court has chosen such a solution and this only in quite specific circumstances: where there was a risk of serious economic repercussions owing in particular to the large number of legal relationships entered into in good faith on the basis of rules considered to be validly in force and where it appeared that individuals and national authorities had been led to adopt practices which did not comply with EU law by reason of objective, significant uncertainty regarding the implications of EU provisions, to which the conduct of other Member States or the Union may even have contributed.[91]

140. In the present case, the information referred to in the order for reference does not make it possible to conclude that a large number of bona fide legal relationships based on the contested provision would have been affected and, consequently, that it would be particularly difficult to ensure *ex tunc* compliance with the preliminary ruling of the Court declaring that provision incompatible with EU law.

141. Accordingly, there is no need to limit the temporal effects of the Court's judgment in the present case.

84 This is commonly referred to as the *ex tunc* effect of preliminary rulings under Article 267 TFEU.

85 See, by way of example, judgments of 29 September 2015, *Gmina Wrocław* (C-276/14, EU:C:2015:635, paragraph 44), and of 28 October 2020, *Bundesrepublik Deutschland (Determination of toll rates for the use of motorways)* (C-321/19, EU:C:2020:866, paragraph 54).

86 See, by way of example, judgments of 29 September 2015, *Gmina Wrocław* (C-276/14, EU:C:2015:635, paragraph 45), and of 28 October 2020, *Bundesrepublik Deutschland (Determination of toll rates for the use of motorways)* (C-321/19, EU:C:2020:866, paragraph 55).

87 See judgments of 8 September 2010, *Winner Wetten* (C-409/06, EU:C:2010:503, paragraph 67), and of 19 November 2009, *Filipiak* (C-314/08, EU:C:2009:719, paragraph 84). See also judgment of 6 March 2007, *Meilicke and Others* (C-292/04, EU:C:2007:132, paragraph 36 and the case-law cited).

88 See judgments of 17 December 1970, *Internationale Handelsgesellschaft* (11/70, EU:C:1970:114, paragraph 3), and of 8 September 2010, *Winner Wetten* (C-409/06, EU:C:2010:503, paragraph 61).

89 See, by way of example, judgments of 29 September 2015, *Gmina Wrocław* (C-276/14, EU:C:2015:635, paragraph 45), and of 28 October 2020, *Bundesrepublik Deutschland (Determination of toll rates for the use of motorways)* (C-321/19, EU:C:2020:866, paragraph 55).

90 See also Lenaerts, K., Maselis, I., Gutman, K., *EU Procedural Law*, Oxford University Press, Oxford, 2014, point 6.34, p. 247.

91 See, by way of example, judgment of 16 September 2020, *Romenergo and Aris Capital* (C-339/19, EU:C:2020:709, paragraph 49 and the case-law cited).

142. I therefore propose to reply to the fourth question that it is not possible to apply the provision at issue and maintain its legal effects until such time as the decision ultimately adopted by the Satversmes tiesa (Constitutional Court) becomes final.

V. Conclusion

143. In the light of the foregoing, I propose that the Court answer the questions referred by the Satversmes tiesa (Constitutional Court, Latvia) as follows:

(1) Article 10 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), is to be interpreted as meaning that it does not cover situations of processing of personal data relating to penalty points recorded against drivers for motoring offences as provided for by a national law such as Article 14^{1} (2) of the Ceļu satiksmes likums (the Law on motoring).

(2) Article 5(1)(c) of Regulation 2016/679 precludes a Member State from processing and communicating personal data relating to penalty points recorded against drivers for motoring offences.

(3) Article 5(1)(b) and (c) of Regulation 2016/679 precludes a Member State from processing and communicating personal data relating to penalty points recorded against drivers for motoring offences when that communication is for the purposes of re-use.

(4) Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information does not govern the processing and communicating, including for the purposes of re-use, of personal data relating to penalty points recorded against drivers for motoring offences.

(5) It is not possible to apply the provision at issue and maintain its legal effects until such time as the decision ultimately adopted by the Satversmes tiesa (Constitutional Court) becomes final.