

Provisional text

## JUDGMENT OF THE COURT (Grand Chamber)

22 June 2021 (\*)

(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Articles 5, 6 and 10 – National legislation providing for public access to personal data relating to penalty points imposed for road traffic offences – Lawfulness – Concept of ‘personal data relating to criminal convictions and offences’ – Disclosure for the purpose of improving road safety – Right of public access to official documents – Freedom of information – Reconciliation with the fundamental rights to respect for private life and to the protection of personal data – Re-use of data – Article 267 TFEU – Temporal effect of a preliminary ruling – Ability of a constitutional court of a Member State to maintain the legal effects of national legislation incompatible with EU law – Principles of primacy of EU law and of legal certainty)

In Case C-439/19,

REQUEST for a preliminary ruling under Article 267 TFEU from the Latvijas Republikas Satversmes tiesa (Constitutional Court, Latvia), made by decision of 4 June 2019, received at the Court on 11 June 2019, in the proceedings brought by

**B**

other party:

**Latvijas Republikas Saeima,**

THE COURT (Grand Chamber),

composed of K. Lenaerts, President, R. Silva de Lapuerta, Vice-President, J.-C. Bonichot, A. Arabadjiev, E. Regan, M. Ilešič (Rapporteur) and N. Piçarra, Presidents of Chambers, E. Juhász, M. Safjan, D. Šváby, S. Rodin, F. Biltgen, K. Jürimäe, C. Lycourgos and P.G. Xuereb, Judges,

Advocate General: M. Szpunar,

Registrar: A. Calot Escobar,

having regard to the written procedure,

after considering the observations submitted on behalf of:

- the Latvian Government, initially by V. Soņeca and K. Pommere, and subsequently by K. Pommere, acting as Agents,
- the Netherlands Government, by M.K. Bulterman and M. Noort, acting as Agents,
- the Austrian Government, by J. Schmoll and G. Kunnert, acting as Agents,
- the Portuguese Government, by L. Inez Fernandes, P. Barros da Costa, A.C. Guerra and I. Oliveira, acting as Agents,

- the Swedish Government, by C. Meyer-Seitz, H. Shev, H. Eklinder, R. Shahsavan Eriksson, A. Runeskjöld, M. Salborn Hodgson, O. Simonsson and J. Lundberg acting as Agents,
  - the European Commission, by D. Nardi, H. Kranenborg and I. Rubene, acting as Agents,
- after hearing the Opinion of the Advocate General at the sitting on 17 December 2020,
- gives the following

## Judgment

- 1 This request for a preliminary ruling concerns the interpretation of Articles 5, 6 and 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) (OJ 2016 L 119, p. 1; ‘the GDPR’), of Article 1(2)(cc) of Directive 2003/98/EC 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) (‘Directive 2003/98’), and of the principles of primacy of EU law and legal certainty.
- 2 The request has been made in proceedings brought by B concerning the legality of national legislation providing for public access to personal data relating to penalty points imposed for road traffic offences.

### Legal context

#### *EU law*

##### *Directive 95/46/EC*

- 3 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31) was repealed by the GDPR, with effect from 25 May 2018. Article 3 of that directive, headed ‘Scope’, was worded as follows:

- ‘1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.
2. This Directive shall not apply to the processing of personal data:
  - in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the [EU Treaty, in the version in force prior to the Treaty of Lisbon,] and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

...’

#### *The GDPR*

- 4 Recitals 1, 4, 10, 16, 19, 39, 50 and 154 of the GDPR state:

- ‘(1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the ‘Charter’) and Article 16(1) [TFEU] provide that everyone has the right to the protection of personal data concerning him or her.
- ...
- (4) The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.
- ...
- (10) In order to ensure a consistent and high level of protection of natural persons and to remove the obstacles to flows of personal data within the Union, the level of protection of the rights and freedoms of natural persons with regard to the processing of such data should be equivalent in all Member States. Consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union. ...
- ...
- (16) This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.
- ...
- (19) 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, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely 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) ... In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. ... Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. ...

...

- (50) The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the 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, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. ...

...

- (154) This Regulation allows the principle of public access to official documents to be taken into account when applying this Regulation. Public access to official documents may be considered to be in the public interest. Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject. Such laws should reconcile public access to official documents and the reuse of public sector information with the right to the protection of personal data and may therefore provide for the necessary reconciliation with the right to the protection of personal data pursuant to this Regulation. The reference to public authorities and bodies should in that context include all authorities or other bodies covered by Member State law on public access to documents. Directive [2003/98/EC] leaves intact and in no way affects the level of protection of natural persons with regard to the processing of personal data under the provisions of Union and Member State law, and in particular does not alter the obligations and rights set out in this Regulation. In particular, that Directive should not apply to documents to which access 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 provided for by law as being incompatible with the law concerning the protection of natural persons with regard to the processing of personal data.'

5 Article 1 of the GDPR, headed 'Subject matter and objectives', provides:

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.
2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.
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.'

6 Article 2 of the GDPR, headed 'Material scope', provides in paragraphs 1 and 2:

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.’

7 As set out in Article 4 of the GDPR, headed ‘Definitions’:

‘For the purposes of this Regulation:

- (1) “personal data” means any information relating to an identified or identifiable natural person ...;
- (2) “processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

...

- (7) “controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

...’

8 Article 5 of the GDPR, headed ‘Principles relating to processing of personal data’, states:

‘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; ... (“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; ... (“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”).’

9 Article 6 of the GDPR, headed ‘Lawfulness of processing’, provides in paragraph 1:

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

- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (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;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (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;
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

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

- 10 Article 10 of the GDPR, headed 'Processing of personal data relating to criminal convictions and offences', provides:

'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.'

- 11 Article 51 of the GDPR, headed 'Supervisory authority', states in paragraph 1:

'Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ("supervisory authority").'

- 12 Article 85 of the GDPR, headed 'Processing and freedom of expression and information', provides in paragraph 1:

'Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression.'

- 13 Article 86 of the GDPR, headed 'Processing and public access to official documents', provides:

'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 Union 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 this Regulation.'

- 14 As set out in Article 87 of the GDPR, headed 'Processing of the national identification number':

‘Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.’

15 Article 94 of the GDPR provides:

- ‘1. Directive [95/46] is repealed with effect from 25 May 2018.
2. References to the repealed Directive shall be construed as references to this Regulation. ...’

*Directive 2016/680*

16 Recitals 10, 11 and 13 of Directive 2016/680 state:

‘(10) In Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which adopted the Treaty of Lisbon, the conference acknowledged that specific rules on the protection of personal data and the free movement of personal data in the fields of judicial cooperation in criminal matters and police cooperation based on Article 16 TFEU may prove necessary because of the specific nature of those fields.

(11) It is therefore appropriate for those fields to be addressed by a directive that lays down the specific rules relating to 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, including the safeguarding against and the prevention of threats to public security, respecting the specific nature of those activities. Such competent authorities may include not only public authorities such as the judicial authorities, the police or other law-enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of this Directive. Where such a body or entity processes personal data for purposes other than for the purposes of this Directive, [the GDPR] applies. [The GDPR] therefore applies in cases where a body or entity collects personal data for other purposes and further processes those personal data in order to comply with a legal obligation to which it is subject. ...

...

(13) A criminal offence within the meaning of this Directive should be an autonomous concept of Union law as interpreted by the Court of Justice of the European Union ...’

17 Article 3 of Directive 2016/680 provides:

‘For the purposes of this Directive:

...

7. “competent authority” means:

- (a) any public authority competent for 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; or
- (b) any other body or entity entrusted by Member State law to exercise public authority and public powers 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;

...’

*Directive 2003/98*

18 Recital 21 of Directive 2003/98 states:

‘This Directive should be implemented and applied in full compliance with the principles relating to the protection of personal data in accordance with Directive [95/46].’

19 Article 1 of Directive 2003/98, headed ‘Subject matter and scope’, provides 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:

...

(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;

...

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

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].

...’

*Latvian law*

20 Article 96 of the Latvijas Republikas Satversme (Constitution of the Republic of Latvia; ‘the Latvian Constitution’) provides:

‘Everyone has the right to respect for his or her private life, home and correspondence.’

21 Under Article 1(5) of the Informācijas atklātības likums (Law on freedom of information) of 29 October 1998 (*Latvijas Vēstnesis*, 1998, No 334/335), re-use consists in the use of publicly accessible information, held and created by an authority, for commercial or non-commercial purposes other than the initial purpose for which the information was created, if that use is by a private party and does not involve tasks in the exercise of public authority.

22 Under Article 4 of that law, publicly accessible information is information that does not fall within the category of information subject to restricted access.

23 Article 5(1) of that law provides that information is subject to restricted access where it is intended for a restricted group of persons for the purpose of the performance of their tasks or professional duties and the disclosure or loss thereof, on account of its nature and content, hinders or may hinder an authority’s activities, or causes or may cause harm to statutorily protected interests of persons. Article 5(2) states that information is regarded as being subject to restricted access where, inter alia, it is so provided by law and Article 5(6) specifies that information that has already been published cannot be regarded as being information subject to restricted access.



24 In accordance with Article 10(3) of the Law on freedom of information, publicly accessible information may be provided upon request. The applicant is not required to justify specifically his or her interest in obtaining the information, and may not be refused access on the ground that the information does not concern him or her.

25 Article 14<sup>1</sup> of the Ceļu satiksmes likums (Law on road traffic) of 1 October 1997 (*Latvijas Vēstnesis*, 1997, No 274/276), in the version applicable at the material time ('the Law on road traffic'), headed 'Access to information kept in the national register of vehicles and their drivers ...', states in paragraph 2:

'Information relating ... to a person's right to drive vehicles, to fines for the commission of road traffic 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 ... shall be regarded as information in the public domain.'

26 Article 43<sup>1</sup> of the Law on road traffic, headed 'Penalty points system', provides in paragraph 1:

'In order to influence the behaviour of drivers of vehicles, by promoting safe driving and compliance with road traffic rules, and in order to reduce as far as possible the risks for human life, human health and a person's property, administrative offences committed by drivers of vehicles shall be entered in the register of convictions and penalty points shall be entered in the national register of vehicles and their drivers.'

27 In accordance with paragraphs 1 and 4 of Ministru kabineta noteikumi Nr. 551 'Pārkāpumu uzskaites punktu sistēmas piemērošanas noteikumi' (Cabinet Regulation No 551 on the rules for application of the penalty points system) of 21 June 2004 (*Latvijas Vēstnesis*, 2004, No 102), penalty points for administrative offences committed in relation to road traffic by drivers of vehicles are automatically registered on the day upon which the period for appealing against the decision imposing an administrative penalty expires.

28 Under paragraph 7 of that regulation, penalty points are removed when they have expired.

29 By virtue of paragraph 12 of that regulation, depending on the number of penalty points, drivers are subject to measures such as warnings, road safety training or tests, or a driving ban for a specified period.

30 As is apparent from Article 32(1) of the Satversmes tiesas likums (Law on the Constitutional Court) of 5 June 1996 (*Latvijas Vēstnesis*, 1996, No 103), a judgment of the Latvijas Republikas Satversmes tiesa (Constitutional Court, Latvia) is final and enforceable when it is delivered. In accordance with Article 32(3) of that law, a legal provision which the Latvijas Republikas Satversmes tiesa (Constitutional Court) has declared to be inconsistent with a higher-ranking rule of law is treated as void from the day of publication of the judgment of that court, unless the court decides otherwise.

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

31 B is a natural person upon whom penalty points were imposed on account of one or more road traffic offences. In accordance with the Law on road traffic and Regulation No 551 of 21 June 2004, the Ceļu satiksmes drošības direkcija (Road Safety Directorate, Latvia) ('the CSDD') entered those penalty points in the national register of vehicles and their drivers.

32 Since the information relating to those penalty points that was contained in the register was accessible to the public and moreover, according to B, had been disclosed, for purposes of re-use, to a number of economic operators, B lodged a constitutional complaint with the Latvijas Republikas Satversmes tiesa (Constitutional Court), in order for it to examine whether Article 14<sup>1</sup>(2) of the Law on road traffic is consistent with the fundamental right to respect for private life laid down in Article 96 of the Latvian Constitution.

- 33 The Latvijas Republikas Saeima (Parliament of the Republic of Latvia; ‘the Latvian Parliament’) was involved in the proceedings as the institution which had adopted the Law on road traffic. In addition, the CSDD, which processes the data relating to penalty points imposed for road traffic offences, was heard, as were the Datu valsts inspekcija (data protection authority), which is the supervisory authority, within the meaning of Article 51 of the GDPR, in Latvia, and a number of other authorities and persons.
- 34 In the context of the main proceedings, the Latvian Parliament confirmed that, under Article 14<sup>1</sup>(2) of the Law on road traffic, any person may obtain information relating to penalty points imposed on another person, either by enquiring directly at the CSDD or by using the services provided by commercial re-users.
- 35 It stated that that provision is lawful because it is justified by the objective of improving road safety. That public interest requires that persons infringing traffic regulations, in particular those disregarding them systematically and in bad faith, be openly identified and that drivers of vehicles, by means of that transparency, be deterred from committing offences.
- 36 Furthermore, that provision is justified by the right of access to information, laid down by the Latvian Constitution.
- 37 The Latvian Parliament explained that, in practice, disclosure of the information contained in the national register of vehicles and their drivers is subject to the condition that the person requesting the information must provide the national identification number of the driver about whom he or she wishes to enquire. This precondition for obtaining information is attributable to the fact that, unlike the person’s name, which may be identical to the name of other persons, the national identification number is a unique identifier.
- 38 The CSDD pointed out that Article 14<sup>1</sup>(2) of the Law on road traffic does not impose any limits on either public access to or re-use of data relating to penalty points. As regards the contracts which it concludes with commercial re-users, the CSDD stated that they do not provide for legal transfer of the data and that re-users must ensure that the information transmitted to their customers does not exceed that which can be obtained from the CSDD. In addition, under those contracts the acquirer affirms that it will use the information obtained in accordance with the purposes indicated in the contract and in compliance with the legislation in force.
- 39 The Datu valsts inspekcija (data protection authority) expressed its doubts as to whether Article 14<sup>1</sup>(2) of the Law on road traffic is consistent with Article 96 of the Latvian Constitution which lays down the right to respect for private life. In its view, the importance and the objective of processing carried out on the basis of the provision at issue in the main proceedings are not clearly established, and it cannot therefore be ruled out that that processing is inappropriate or disproportionate. Whilst the statistics relating to road traffic accidents in Latvia show a decrease in the number of accidents, there is, however, no proof that the penalty points system and public access to information relating to it have contributed to that favourable development.
- 40 The Latvijas Republikas Satversmes tiesa (Constitutional Court) notes, first of all, that the constitutional complaint concerns Article 14<sup>1</sup>(2) of the Law on road traffic only in so far as that provision makes penalty points entered in the national register of vehicles and their drivers accessible to the public.
- 41 It observes, next, that penalty points are personal data and that, when assessing the right to respect for private life laid down in Article 96 of the Latvian Constitution, account is to be taken of the GDPR and, more generally, of Article 16 TFEU and Article 8 of the Charter.
- 42 As regards the objectives of the Latvian road traffic legislation, that court explains that it is in particular in order to promote road safety that offences committed by drivers, which are classified as administrative offences in Latvia, are entered in the register of convictions and that penalty points are entered in the national register of vehicles and their drivers.

- 43 So far as concerns, in particular, the national register of vehicles and their drivers, it states that that register enables the number of road traffic offences committed to be ascertained and measures to be implemented in the light of their number. The system relating to penalty points entered in that register is thus intended to improve road safety, first, by enabling drivers of vehicles who disregard the road traffic rules systematically and in bad faith to be distinguished from drivers who commit offences occasionally. Second, such a system is also capable of influencing the conduct of road users in a preventive manner, by encouraging them to comply with the road traffic rules.
- 44 That court observes that it is not in dispute that Article 14<sup>1</sup>(2) of the Law on road traffic grants any person the right to request and obtain from the CSDD the information contained in the national register of vehicles and their drivers concerning the penalty points imposed on drivers. It confirms that, in practice, the information is provided to the person requesting it once that person indicates the national identification number of the driver concerned.
- 45 The Latvijas Republikas Satversmes tiesa (Constitutional Court) then explains that, since penalty points are classified as publicly accessible information, they fall within the scope of the Law on freedom of information and that that information may therefore be re-used for commercial or non-commercial purposes other than the initial purpose for which the information was created.
- 46 In order to interpret and apply Article 96 of the Latvian Constitution consistently with EU law, that court seeks to ascertain, first, whether information relating to penalty points is among the information referred to in Article 10 of the GDPR, that is to say, ‘personal data relating to criminal convictions and offences’. If it is, the view could be taken that Article 14<sup>1</sup>(2) of the Law on road traffic fails to comply with the requirement contained in Article 10 of the GDPR that processing of the data to which that article relates can take place only ‘under the control of official authority’ or if there are ‘appropriate safeguards for the rights and freedoms of data subjects’.
- 47 That court states that Article 8(5) of Directive 95/46, which left it to each Member State to determine whether the special rules on data relating to offences and criminal convictions should be extended to data relating to administrative offences and sanctions, was, from 1 September 2007, implemented in Latvia in such a way that 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.
- 48 It adds that the scope of Article 10 of the GDPR must, in accordance with recital 4 of that regulation, be assessed in the light of the function of fundamental rights in society. In that respect, the objective of preventing a previous conviction from having an excessive adverse effect on a person’s private and professional life could apply both to criminal convictions and to administrative offences. Account should be taken, in this context, of the case-law of the European Court of Human Rights on the equiparation of certain administrative cases with criminal cases.
- 49 The Latvijas Republikas Satversmes tiesa (Constitutional Court) raises, second, the question of the scope of Article 5 of the GDPR. It is unsure, in particular, whether the Latvian legislature has complied with the obligation, set out in Article 5(1)(f), requiring personal data to be processed with ‘integrity and confidentiality’. It points out that Article 14<sup>1</sup>(2) of the Law on road traffic, which, by giving access to information relating to penalty points, makes it possible to ascertain whether a person has been found guilty of a road traffic offence, was not accompanied by specific measures ensuring the security of such data.
- 50 That court seeks, third, to ascertain whether Directive 2003/98 is relevant when examining whether Article 14<sup>1</sup>(2) of the Law on road traffic is compatible with the right to respect for private life. It is apparent from that directive that the re-use of personal data may be permitted only if that right is respected.
- 51 Fourth, in the light of the Court of Justice’s case-law according to which the interpretation of EU law provided in preliminary rulings has *erga omnes* and *ex tunc* effects, the Latvijas Republikas Satversmes

tiesa (Constitutional Court) is uncertain whether, if Article 14<sup>1</sup>(2) of the Law on road traffic were to be incompatible with Article 96 of the Latvian Constitution, read in the light of the GDPR and the Charter, it could nevertheless maintain the temporal effects of Article 14<sup>1</sup>(2) of that law until the date of delivery of its judgment, given the large number of legal relationships at issue.

52 It states that, under Latvian law, a measure that it declares unconstitutional is to be considered void from the day of delivery of its judgment, unless it decides otherwise. It explains that it must, in that regard, strike a balance between the principle of legal certainty and the fundamental rights of the various parties concerned.

53 In those circumstances, the Latvijas Republikas Satversmes tiesa (Constitutional Court) decided to stay the proceedings and to refer the following questions to the Court of Justice 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 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 [the Satversmes tiesa (Constitutional Court) makes a final ruling]?’

## **Consideration of the questions referred**

### ***First question***

54 By its first question, the referring court asks, in essence, whether Article 10 of the GDPR must be interpreted as applying to the processing of personal data relating to penalty points imposed on drivers of vehicles for road traffic offences, consisting in the public disclosure of such data.

55 Under Article 10 of the GDPR, processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) is to be carried out only under the control of official authority or when the processing is authorised by EU or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

56 It should, therefore, first of all be determined whether the information relating to penalty points that is disclosed to third parties pursuant to the legislation at issue in the main proceedings constitutes ‘personal data’, within the meaning of Article 4(1) of the GDPR, and whether that disclosure constitutes ‘processing’ of such data, within the meaning of Article 4(2) of that regulation, that comes under its material scope as defined in Article 2.

- 57 In the first place, it is apparent from the order for reference that Latvian legislation provides for the imposition of penalty points on drivers of vehicles who have committed a road traffic offence and upon whom a financial or other penalty has been imposed. Those points are entered by a public body, the CSDD, in the national register of vehicles and their drivers on the day upon which the period for appealing against the decision imposing that penalty expires.
- 58 It is also apparent from the order for reference that road traffic offences and the penalties for punishing them fall within administrative law in Latvia and that the aim of imposing penalty points is not to inflict a further penalty but to heighten awareness of the drivers concerned, by encouraging them to adopt safer driving behaviour. When a certain number of penalty points is reached, the person concerned may be banned from driving for a specified period.
- 59 It is, in addition, clear from the order for reference that the legislation at issue in the main proceedings obliges the CSDD to disclose information relating to the penalty points imposed on a given driver to any person who requests access to that information. The CSDD merely requires, for that purpose, that the person seeking the information duly identifies the driver concerned by providing his or her national identification number.
- 60 It must therefore be found that the information relating to penalty points, which concerns an identified natural person, is ‘personal data’, within the meaning of Article 4(1) of the GDPR, and that its disclosure by the CSDD to third parties constitutes ‘processing’, within the meaning of Article 4(2) of the GDPR.
- 61 In the second place, the disclosure of that information falls within the very broad definition, set out in Article 2(1), of the GDPR’s material scope and is not included in the processing of personal data that Article 2(2)(a) and (d) of the GDPR excludes from its material scope.
- 62 First, Article 2(2)(a) of the GDPR provides that that regulation does not apply to the processing of personal data ‘in the course of an activity which falls outside the scope of Union law’. That exception to the applicability of the GDPR must, like the other exceptions laid down in Article 2(2), be interpreted strictly (see, to that effect, judgments of 9 July 2020, *Land Hessen*, C-272/19, EU:C:2020:535, paragraph 68, and of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559, paragraph 84).
- 63 In that regard, Article 2(2)(a) of the GDPR is to be read in conjunction with Article 2(2)(b) thereof and recital 16, which states that that regulation does not apply to the processing of personal data in the context of ‘activities which fall outside the scope of Union law, such as activities concerning national security’ and ‘activities in relation to the common foreign and security policy of the Union’.
- 64 It follows that Article 2(2)(a) and (b) of the GDPR represents partly a continuation of the first indent of Article 3(2) of Directive 95/46. Therefore, Article 2(2)(a) and (b) of the GDPR cannot be interpreted in broader terms than the exception resulting from the first indent of Article 3(2) of Directive 95/46, a provision which already excluded from that directive’s scope inter alia the processing of personal data taking place in the course ‘of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the [EU Treaty, in the version in force prior to the Treaty of Lisbon,] and in any case ... processing operations concerning public security, defence, State security ...’.
- 65 As the Court has repeatedly held, only the processing of personal data in the course of an activity of the State or of State authorities which was expressly listed in Article 3(2) of Directive 95/46 or in the course of an activity which could be classified in the same category was excluded from the scope of that directive (see, to that effect, judgments of 6 November 2003, *Lindqvist*, C-101/01, EU:C:2003:596, paragraphs 42 to 44; of 27 September 2017, *Puškár*, C-73/16, EU:C:2017:725, paragraphs 36 and 37; and of 10 July 2018, *Jehovan todistajat*, C-25/17, EU:C:2018:551, paragraph 38).
- 66 It follows that Article 2(2)(a) of the GDPR, read in the light of recital 16 thereof, must be regarded as being designed solely to exclude from the scope of that regulation the processing of personal data carried

out by State authorities in the course of an activity which is intended to safeguard national security or of an activity which can be classified in the same category, with the result that the mere fact that an activity is an activity characteristic of the State or of a public authority is not sufficient ground for that exception to be automatically applicable to such an activity (see, to that effect, judgment of 9 July 2020, *Land Hessen*, C-272/19, EU:C:2020:535, paragraph 70).

67 The activities having the aim of safeguarding national security that are envisaged in Article 2(2)(a) of the GDPR encompass, in particular, as the Advocate General has also observed in essence in points 57 and 58 of his Opinion, those that are intended to protect essential State functions and the fundamental interests of society.

68 However, activities relating to road safety do not pursue such an objective and consequently cannot be classified in the category of activities having the aim of safeguarding national security, which are envisaged in Article 2(2)(a) of the GDPR.

69 Second, Article 2(2)(d) of the GDPR provides that that regulation does not apply 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, including the safeguarding against and the prevention of threats to public security’. As is clear from recital 19 of the GDPR, the reason for that exception is that the processing of personal data for such purposes by the competent authorities is governed by a more specific EU legal act, namely Directive 2016/680, which was adopted on the same day as the GDPR. Directive 2016/680 defines ‘competent authority’ in Article 3(7) and such a definition must be applied, by analogy, to Article 2(2)(d) of the GDPR.

70 It is apparent from recital 10 of Directive 2016/680 that the concept of ‘competent authority’ must be understood in relation to the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, in view of the arrangements which may prove necessary, in that regard, because of the specific nature of those fields. In addition, recital 11 of that directive explains that the GDPR applies to processing of personal data that is carried out by a ‘competent authority’, within the meaning of Article 3(7) of the directive, but for purposes other than those of the directive.

71 In the light of the material available to the Court, it does not appear that, in carrying out the activities at issue in the main proceedings, which consist in disclosing to the public, for a road safety purpose, personal data relating to penalty points, the CSDD may be regarded as a ‘competent authority’, within the meaning of Article 3(7) of Directive 2016/680, and, therefore, that such activities may be covered by the exception laid down in Article 2(2) of the GDPR.

72 Therefore, the disclosure by the CSDD of the personal data relating to penalty points imposed on drivers of vehicles for road traffic offences falls within the material scope of the GDPR.

73 As to the applicability of Article 10 of the GDPR to such disclosure, the question is whether the information thereby disclosed constitutes personal data ‘relating to criminal convictions and offences or related security measures’, within the meaning of that provision, the processing of which ‘shall be carried out only under the control of official authority’, unless the processing is ‘authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects’.

74 In that regard, it is to be noted that Article 10 of the GDPR is intended to ensure enhanced protection as regards processing which, because of the particular sensitivity of the data at issue, is liable to constitute a particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data, guaranteed by Articles 7 and 8 of the Charter (see, to that effect, judgment of 24 September 2019, *GC and Others (De-referencing of sensitive data)*, C-136/17, EU:C:2019:773, paragraph 44).

75 Since the data to which Article 10 of the GDPR refers relates to behaviour that gives rise to social disapproval, the grant of access to such data is liable to stigmatise the data subject and thereby to constitute

a serious interference with his or her private or professional life.

- 76 In the present instance, it is true that decisions of the Latvian authorities for the purpose of punishment of road traffic offences are, as the Latvian Government has stated in its replies to the Court's questions, entered in the register of convictions, to which the public has access only in limited circumstances, and not in the register of vehicles and their drivers, to which Article 14<sup>1</sup>(2) of the Law on road traffic gives free access. However, as the referring court pointed out, disclosure by the CSDD of personal data entered in the latter register that relate to penalty points enables the public to ascertain whether a given person has committed road traffic offences and, if so, to deduce the seriousness and frequency of those offences. Such a system for the disclosure of penalty points therefore effectively gives access to personal data relating to road traffic offences.
- 77 In order to determine whether such access amounts to processing of personal data relating to 'offences', within the meaning of Article 10 of the GDPR, it must be pointed out, first, that that term refers exclusively to criminal offences, as is apparent *inter alia* from the history of the GDPR. Whilst the European Parliament had proposed the express inclusion in that provision of the words 'administrative sanctions' (OJ 2017 C 378, p. 430), that proposal was not adopted. That fact is all the more noteworthy because the provision that preceded Article 10 of the GDPR, namely Article 8(5) of Directive 95/46, which referred, in its first subparagraph, to 'offences' and 'criminal convictions', enabled the Member States, in its second subparagraph, to 'provide that data relating to administrative sanctions ... also be processed under the control of official authority'. It is thus clear from reading Article 8(5) as a whole that the term 'offence' referred only to criminal offences.
- 78 Accordingly, it must be held that, in deliberately not including the adjective 'administrative' in Article 10 of the GDPR, the EU legislature intended to limit the enhanced protection provided for by that provision to the criminal field alone.
- 79 As the Advocate General has observed in points 74 to 77 of his Opinion, that interpretation is borne out by the fact that a number of language versions of Article 10 of the GDPR make express reference to 'criminal offences', for example the versions in German (*Straftaten*), Spanish (*infracciones penales*), Italian (*reati*), Lithuanian (*nusikalstamas veikas*), Maltese (*reati*) and Dutch (*strafbare feiten*).
- 80 Second, the fact that road traffic offences are classified as administrative in Latvia is not decisive when determining whether those offences are covered by Article 10 of the GDPR.
- 81 In that regard, it should be pointed out that the terms 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 (judgments of 19 September 2000, *Linster*, C-287/98, EU:C:2000:468, paragraph 43, and of 1 October 2019, *Planet49*, C-673/17, EU:C:2019:801, paragraph 47).
- 82 In the present instance, it is to be noted, first of all, that the GDPR does not contain any reference to national law so far as concerns the scope of the terms in Article 10 thereof, in particular the terms 'offences' and 'criminal convictions'.
- 83 Next, it is apparent from recital 10 of the GDPR that that regulation is intended to contribute to the accomplishment of an area of freedom, security and justice by ensuring a consistent and high level of protection of natural persons with regard to the processing of personal data, which requires the level of protection to be equivalent and homogeneous in all the Member States. It would be contrary to such an objective if the enhanced protection provided for in Article 10 of the GDPR applied to the processing of personal data relating to road traffic offences only in some Member States, and not in others, solely because those offences are not classified as criminal in the latter Member States.
- 84 Finally, as the Advocate General has observed in point 84 of his Opinion, that finding is supported by recital 13 of Directive 2016/680 which states that 'a criminal offence within the meaning of this Directive

should be an autonomous concept of Union law as interpreted by the Court of Justice of the European Union’.

- 85 It follows that the concept of ‘criminal offence’, which is decisive for determining whether Article 10 of the GDPR is applicable to personal data relating to road traffic offences, such as the data at issue in the main proceedings, requires an autonomous and uniform interpretation throughout the European Union, having regard to the objective pursued by that provision and the context of which it forms part; the classification given by the Member State concerned to those offences is not conclusive in that regard as the classification may vary from one country to another (see, to that effect, judgment of 14 November 2013, *Baláž*, C-60/12, EU:C:2013:733, paragraphs 26 and 35).
- 86 Third, it must be examined whether road traffic offences, such as those which give rise to entry in the register of vehicles and their drivers of the penalty points whose disclosure to third parties is provided for by the provision at issue, constitute a ‘criminal offence’, for the purposes of Article 10 of the GDPR.
- 87 According to the Court’s case-law, three criteria are relevant for assessing whether an offence is criminal in nature. The first criterion is the legal classification of the offence under national law, the second is the intrinsic nature of the offence, and the third is the degree of severity of the penalty that the person concerned is liable to incur (see, to that effect, judgments of 5 June 2012, *Bonda*, C-489/10, EU:C:2012:319, paragraph 37; of 20 March 2018, *Garlsson Real Estate and Others*, C-537/16, EU:C:2018:193, paragraph 28; and of 2 February 2021, *Consob*, C-481/19, EU:C:2021:84, paragraph 42).
- 88 Even in the case of offences which are not classified as ‘criminal’ by national law, the intrinsic nature of the offence in question and the degree of severity of the penalties to which it is liable to give rise may nevertheless result in its being criminal in nature (see, to that effect, judgment of 20 March 2018, *Garlsson Real Estate and Others*, C-537/16, EU:C:2018:193, paragraphs 28 and 32).
- 89 As regards the criterion relating to the intrinsic nature of the offence, it must be ascertained whether the penalty at issue has a punitive purpose and the mere fact that it also pursues a deterrent purpose does not mean that it cannot be characterised as a criminal penalty. It is of the very nature of criminal penalties that they seek both to punish and to deter unlawful conduct. By contrast, a measure which merely repairs the damage caused by the offence at issue is not criminal in nature (see, to that effect, judgments of 5 June 2012, *Bonda*, C-489/10, EU:C:2012:319, paragraph 39, and of 20 March 2018, *Garlsson Real Estate and Others*, C-537/16, EU:C:2018:193, paragraph 33). It is not in dispute that the giving of penalty points for road traffic offences, and also the fines or other penalties to which the commission of those offences may give rise, are not intended only to repair any harm caused by those offences but also have a punitive purpose.
- 90 So far as concerns the criterion relating to the degree of severity of the penalties to which the commission of those offences may give rise, it is to be noted, first of all, that only road traffic offences of a certain seriousness entail the giving of penalty points and that such offences are therefore liable to give rise to penalties of a certain severity. Next, the imposition of penalty points is generally additional to the penalty for the commission of such an offence, which, as has been noted in paragraph 58 above, is indeed true of the legislation at issue in the main proceedings. Finally, the accumulation of penalty points itself has legal consequences, such as the obligation to sit a test, or even a driving ban.
- 91 This analysis is borne out by the case-law of the European Court of Human Rights according to which, notwithstanding the move towards ‘decriminalisation’ of road traffic offences in certain States, those offences must generally, in the light of the purpose, both deterrent and punitive, of the penalties imposed and the degree of severity that those penalties may have, be regarded as being criminal in nature (see, to that effect, ECtHR, 21 February 1984, *Öztürk v. Germany*, CE:ECHR:1984:0221JUD000854479, §§ 49 to 53; 29 June 2007, *O’Halloran and Francis v. the United Kingdom*, CE:ECHR:2007:0629JUD001580902, §§ 33 to 36; and 4 October 2016, *Rivard v. Switzerland*, CE:ECHR:2016:1004JUD002156312, §§ 23 and 24).



- 92 The classification of road traffic offences which may result in the giving of penalty points as a ‘criminal offence’, for the purposes of Article 10 of the GDPR, is also consonant with the aim of that provision. The public disclosure of personal data relating to road traffic offences, including the penalty points imposed for committing them, is liable, in light of the fact that such offences compromise road safety, to give rise to social disapproval and to result in stigmatisation of the data subject, in particular where the penalty points reveal a certain seriousness or certain frequency of the offences.
- 93 It follows that road traffic offences which may result in penalty points being given are covered by the term ‘offences’ in Article 10 of the GDPR.
- 94 In the light of all the foregoing considerations, the answer to the first question referred is that Article 10 of the GDPR must be interpreted as applying to the processing of personal data relating to penalty points imposed on drivers of vehicles for road traffic offences.

### ***Second question***

- 95 By its second question, the referring court asks, in essence, whether the provisions of the GDPR must be interpreted as precluding national legislation which obliges the public body responsible for the register in which penalty points imposed on drivers of vehicles for road traffic offences are entered to disclose those data to any person who requests them, without that person having to establish a specific interest in obtaining the data.
- 96 All processing of personal data must comply, first, with the principles relating to processing of data set out in Article 5 of the GDPR and, second, with one of the principles relating to lawfulness of processing listed in Article 6 of that regulation (see, to that effect, judgment of 16 January 2019, *Deutsche Post*, C-496/17, EU:C:2019:26, paragraph 57 and the case-law cited).
- 97 As regards the principles relating to processing of personal data, it is true that the referring court makes specific reference to the principles of ‘integrity’ and ‘confidentiality’ laid down in Article 5(1)(f) of the GDPR. Nevertheless, it is apparent from the doubts expressed by that court that it seeks to establish more generally whether the processing of personal data at issue in the main proceedings may be regarded as lawful in the light of all of the provisions of that regulation and, in particular, in the light of the principle of proportionality.
- 98 It follows that account should also be taken, in the answer to be provided to the referring court, of the other principles set out in Article 5(1) of the GDPR, in particular of the principle of ‘data minimisation’ in Article 5(1)(c), according to which personal data are to be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, and which gives expression to the principle of proportionality (see, to that effect, judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, EU:C:2019:1064, paragraph 48).
- 99 So far as concerns the principles relating to lawfulness of processing, Article 6 of the GDPR sets out an exhaustive and restrictive list of the cases in which processing of personal data can be regarded as lawful. Thus, in order to be capable of being considered lawful, processing must fall within one of the cases provided for in Article 6 (see, to that effect, judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, EU:C:2019:1064, paragraphs 37 and 38). The processing of personal data at issue in the main proceedings – namely the public disclosure of data relating to penalty points imposed for road traffic offences – carried out by the CSDD may fall within Article 6(1)(e) of the GDPR, under which processing is lawful if and to the extent that it 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’.
- 100 Furthermore, since, as has been held in paragraph 94 above, personal data relating to penalty points imposed on drivers of vehicles for road traffic offences are covered by Article 10 of the GDPR, their processing is subject to the additional restrictions laid down in that provision. Thus, under that provision, processing of those data ‘shall be carried out only under the control of official authority’, unless it is

‘authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects’. Article 10 states, in addition, that ‘any comprehensive register of criminal convictions shall be kept only under the control of official authority’.

101 In the present instance, it is not in dispute that the processing of personal data at issue in the main proceedings, namely the public disclosure of data relating to penalty points imposed for road traffic offences, is carried out by a public body, the CSDD, which is the controller within the meaning of Article 4(7) of the GDPR (see, by analogy, judgment of 9 March 2017, *Manni*, C-398/15, EU:C:2017:197, paragraph 35). However, it is also not in dispute that, once the data have been disclosed, they are consulted by the persons who requested their disclosure and, as the case may be, are stored or disseminated by those persons. Since that further data processing is no longer carried out ‘under the control’ of the CSDD or other official authority, the national law authorising disclosure of the data by the CSDD must provide for ‘appropriate safeguards for the rights and freedoms of data subjects’.

102 Therefore, it is in the light both of the general rules governing lawfulness, in particular those laid down in Article 5(1)(c) and Article 6(1)(e) of the GDPR, and of the specific restrictions prescribed in Article 10 thereof that it should be examined whether national legislation such as that at issue in the main proceedings is consistent with that regulation.

103 In that regard, it is to be noted that none of those provisions lays down a general and absolute prohibition preventing a public authority from being empowered, or indeed compelled, under national legislation to disclose personal data to persons requesting such data.

104 Whilst Article 5(1)(c) of the GDPR requires the principle of ‘data minimisation’ to be observed when personal data are processed, it is clear from the wording of that provision that it is not intended to impose a general and absolute prohibition of that kind and that, in particular, it does not preclude personal data from being disclosed to the public where such disclosure is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, within the meaning of Article 6(1)(e) of that regulation. That is so even where the data in question are covered by Article 10 of the GDPR, provided that the legislation authorising the disclosure provides for appropriate safeguards for the rights and freedoms of data subjects (see, to that effect, judgment of 24 September 2019, *GC and Others (De-referencing of sensitive data)*, C-136/17, EU:C:2019:773, paragraph 73).

105 In that context, it should be borne in mind that the fundamental rights to respect for private life and to the protection of personal data are not absolute rights, but must be considered in relation to their function in society and be weighed against other fundamental rights. Limitations may therefore be imposed, so long as, in accordance with Article 52(1) of the Charter, they are provided for by law, respect the essence of the fundamental rights and observe the principle of proportionality. Under the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others. They must apply only in so far as is strictly necessary and the legislation which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question (see, to that effect, judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, EU:C:2020:559, paragraphs 172 to 176).

106 Therefore, in order to determine whether public disclosure of personal data relating to penalty points, such as the disclosure at issue in the main proceedings, is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, within the meaning of Article 6(1)(e) of the GDPR, and whether the legislation authorising such disclosure provides for appropriate safeguards for the rights and freedoms of data subjects, within the meaning of Article 10 of that regulation, it should be ascertained in particular whether, having regard to the seriousness of the interference with the fundamental rights to respect for private life and to the protection of personal data caused by that disclosure, the latter is justified, and in particular proportionate, for the purpose of achieving the objectives pursued.

- 107 In the present instance, the Latvian Parliament, in its observations before the referring court, and the Latvian Government, in its observations before the Court of Justice, contend that the disclosure by the CSDD of personal data relating to penalty points to any person who so requests falls within the task in the public interest, entrusted to that body, of improving road safety and is intended, in that respect, in particular to enable identification of drivers of vehicles who systematically infringe the road traffic rules and to influence the conduct of road users by encouraging them to behave in accordance with those rules.
- 108 The improvement of road safety is an objective of general interest recognised by the European Union (see, to that effect, judgment of 23 April 2015, *Aykul*, C-260/13, EU:C:2015:257, paragraph 69 and the case-law cited). Member States are therefore justified in classifying road safety as a ‘task carried out in the public interest’, within the meaning of Article 6(1)(e) of the GDPR.
- 109 However, in order to satisfy the conditions imposed by that provision, it is necessary that the disclosure of personal data relating to penalty points entered in the register kept by the CSDD genuinely meets the objective of general interest of improving road safety, without going beyond what is necessary in order to achieve that objective.
- 110 As recital 39 of the GDPR makes clear, that requirement of necessity is not met where the objective of general interest pursued can reasonably be achieved just as effectively by other means less restrictive of the fundamental rights of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed in Articles 7 and 8 of the Charter, since derogations and limitations in relation to the principle of protection of such data must apply only in so far as is strictly necessary (see, to that effect, judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, EU:C:2019:1064, paragraphs 46 and 47).
- 111 As is clear from the practice of the Member States, each of them has a large number of methods, including that of deterrent punishment of road traffic offences, in particular by depriving the drivers concerned of the right to drive a vehicle, a ban whose breach may in turn be punished by effective sentences, without the public disclosure of the adoption of such measures being necessary. It is also clear from the Member States’ practice that numerous preventive measures may, furthermore, be adopted, ranging from public awareness campaigns to the adoption of individual measures requiring a driver to undergo training and take tests, without the public disclosure of the adoption of such individual measures being necessary. However, it is not apparent from the documents before the Court that such measures had been examined and preferred by the Latvian legislature instead of the adoption of the rules at issue in the main proceedings.
- 112 Furthermore, as has been pointed out in paragraph 92 above, the public disclosure of personal data relating to road traffic offences, including data relating to the penalty points imposed for committing them, is liable to constitute a serious interference with the fundamental rights to respect for private life and to the protection of personal data, since it may give rise to social disapproval and result in stigmatisation of the data subject.
- 113 In the light, first, of the sensitivity of the data in question and the seriousness of that interference with the fundamental rights of data subjects to respect for private life and to the protection of personal data and, second, of the fact that, having regard to the findings in paragraph 111 above, it is not apparent that the objective of improving road safety cannot reasonably be achieved just as effectively by other less restrictive means, the necessity, in order to achieve that objective, of such a system of disclosure of personal data relating to penalty points imposed for road traffic offences cannot be regarded as established (see, by analogy, judgment of 9 November 2010, *Volker und Markus Schecke and Eifert*, C-92/09 and C-93/09, EU:C:2010:662, paragraph 86).
- 114 Thus, whilst it may be justified to distinguish drivers who disregard the road traffic rules systematically and in bad faith from drivers who commit offences occasionally, the view cannot, however, be taken that identification of the first category of drivers must, for the purpose of improving road safety, be carried out by or shared with the general public, with the result that it is even questionable whether the legislation at

issue in the main proceedings is appropriate for achieving the first of the objectives referred to in paragraph 107 above.

- 115 Moreover, it is apparent from the documents before the Court that the CSDD discloses to the public not only the data relating to penalty points imposed on drivers disregarding the road traffic rules systematically and in bad faith, but also the data relating to penalty points imposed on drivers committing offences occasionally. It is thus clear that, in providing for general public access to penalty points, the legislation at issue in the main proceedings in any event goes beyond what is necessary in order to achieve the objective of combatting the systematic disregard in bad faith of the road traffic rules.
- 116 So far as concerns the second objective mentioned in paragraph 107 above pursued by the legislation at issue in the main proceedings, it is apparent from the documents before the Court that, whilst a downward trend in the number of road traffic accidents may have been observed in Latvia, there is no basis for concluding that that trend is connected with disclosure of the information relating to penalty points rather than to the establishment of the penalty points system in itself.
- 117 The conclusion set out in paragraph 113 above is not invalidated by the fact that in practice the CSDD makes disclosure of the personal data at issue conditional on applicants stating the national identification number of the driver about whom they wish to enquire.
- 118 Even if, as the Latvian Government has stated, the disclosure of national identification numbers by the public bodies keeping the population registers is subject to strict requirements and thus complies with Article 87 of the GDPR, the fact remains that the legislation at issue in the main proceedings, as applied by the CSDD, permits any person who knows the national identification number of a particular driver to obtain, without any further condition, the personal data relating to the penalty points that have been imposed on that driver. Such a disclosure regime is liable to lead to a situation in which those data are disclosed to persons who, for reasons unrelated to the objective of general interest of improving road safety, wish to find out about the penalty points that have been imposed on a given person.
- 119 Nor is the conclusion set out in paragraph 113 above invalidated by the fact that the national register of vehicles and their drivers is an official document, within the meaning of Article 86 of the GDPR.
- 120 Whilst, as follows from recital 154 of the GDPR, public access to official documents constitutes a public interest capable of justifying the disclosure of personal data contained in such documents, that access must nevertheless be reconciled with the fundamental rights to respect for private life and to the protection of personal data, as Article 86 indeed expressly requires. In the light in particular of the sensitivity of data relating to penalty points imposed for road traffic offences and of the seriousness of the interference with the fundamental rights of data subjects to respect for private life and to the protection of personal data, which is caused by the disclosure of such data, it must be held that those rights prevail over the public's interest in having access to official documents, in particular the national register of vehicles and their drivers.
- 121 Furthermore, for the same reason, the right to freedom of information referred to in Article 85 of the GDPR cannot be interpreted as justifying the disclosure to any person who so requests of personal data relating to penalty points imposed for road traffic offences.
- 122 In the light of all the foregoing, the answer to the second question is that the provisions of the GDPR, in particular Article 5(1), Article 6(1)(e) and Article 10 thereof, must be interpreted as precluding national legislation which obliges the public body responsible for the register in which penalty points imposed on drivers of vehicles for road traffic offences are entered to make those data accessible to the public, without the person requesting access having to establish a specific interest in obtaining the data.

### ***Third question***

- 123 By its third question, the referring court asks, in essence, whether the provisions of the GDPR, in particular Article 5(1)(b) and Article 10 thereof, and Article 1(2)(cc) of Directive 2003/98 must be interpreted as precluding national legislation which authorises the public body responsible for the register in which penalty points imposed on drivers of vehicles for road traffic offences are entered to disclose those data to economic operators for re-use.
- 124 As the referring court states, this question arises from the fact that the CSDD concludes contracts with economic operators pursuant to which it transmits to them the personal data relating to penalty points entered in the national register of vehicles and their drivers, in order, inter alia, to enable any person wishing to find out about the penalty points imposed on a particular driver to obtain such data not only from the CSDD but also from those economic operators.
- 125 It is clear from the answer to the second question that the provisions of the GDPR, in particular Article 5(1), Article 6(1)(e) and Article 10 thereof, must be interpreted as precluding national legislation which obliges the public body responsible for the register in which penalty points imposed on drivers of vehicles for road traffic offences are entered to make those data accessible to the public, without the person requesting access having to establish a specific interest in obtaining the data.
- 126 Those provisions must, for reasons identical to those set out in the answer to the second question, be interpreted as also precluding national legislation which authorises a public body to disclose data of that kind to economic operators in order for the data to be re-used and disclosed to the public by them.
- 127 Finally, so far as concerns Article 1(2)(cc) of Directive 2003/98, to which the third question also refers, as the Advocate General has observed in points 128 and 129 of his Opinion that provision is not relevant for the purpose of determining whether the rules of EU law on the protection of personal data preclude legislation such as that at issue in the main proceedings.
- 128 Irrespective of whether data relating to penalty points imposed on drivers for road traffic offences are covered by Directive 2003/98, the scope of the protection of those data must, in any event, be determined on the basis of the GDPR, as follows, first, from recital 154 of the GDPR and, second, from recital 21 and Article 1(4) of that directive, both read in conjunction with Article 94(2) of the GDPR. Article 1(4) of Directive 2003/98 provides, in essence, that that directive leaves intact and in no way affects the level of protection of individuals with regard to the processing of personal data inter alia under EU law, and in particular does not alter the obligations and rights set out in the GDPR.
- 129 In the light of the foregoing, the answer to the third question is that the provisions of the GDPR, in particular Article 5(1), Article 6(1)(e) and Article 10 thereof, must be interpreted as precluding national legislation which authorises the public body responsible for the register in which penalty points imposed on drivers of vehicles for road traffic offences are entered to disclose those data to economic operators for re-use.

#### ***Fourth question***

- 130 By its fourth question, the referring court asks, in essence, whether the principle of primacy of EU law must be interpreted as precluding the constitutional court of a Member State, before which a complaint has been brought challenging national legislation that proves, in the light of a preliminary ruling given by the Court of Justice, to be incompatible with EU law, from deciding, in accordance with the principle of legal certainty, that the legal effects of that legislation be maintained until the date of delivery of the judgment by which it rules finally on that constitutional complaint.
- 131 As is apparent from the order for reference, this question has been referred on account of the large number of legal relationships affected by the national legislation at issue in the main proceedings and of the fact that, under Article 32(3) of the Law on the Constitutional Court and the case-law relating thereto, the referring court, in performing its task of ensuring a balance between the principle of legal certainty and the

fundamental rights of the persons concerned, may limit the retroactive effect of its judgments in order to prevent them from seriously compromising the rights of others.

- 132 In that regard, it should be recalled that the interpretation which, in the exercise of the jurisdiction conferred on it by Article 267 TFEU, the Court gives to rules of EU law clarifies and defines the meaning and scope of those rules as they must be or ought to have been understood and applied from the time of their entry into force. It is only exceptionally that the Court 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. 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 (judgments of 6 March 2007, *Meilicke*, C-292/04, EU:C:2007:132, paragraphs 34 and 35; of 22 January 2015, *Balazs*, C-401/13 and C-432/13, EU:C:2015:26, paragraphs 49 and 50; and of 29 September 2015, *Gmina Wrocław*, C-276/14, EU:C:2015:635, paragraphs 44 and 45).
- 133 As the Court has consistently held, such a restriction may be allowed only in the actual judgment ruling upon the interpretation sought. Indeed, there must necessarily be a single occasion when a decision is made on the temporal effects of the requested interpretation which the Court gives of a provision of EU law. The principle that a restriction may be allowed only in the actual judgment ruling upon that interpretation guarantees the equal treatment of the Member States and of other persons subject to EU law, under that law, and fulfils, at the same time, the requirements arising from the principle of legal certainty (judgment of 6 March 2007, *Meilicke*, C-292/04, EU:C:2007:132, paragraphs 36 and 37; see, to that effect, judgments of 23 October 2012, *Nelson and Others*, C-581/10 and C-629/10, EU:C:2012:657, paragraph 91, and of 7 November 2018, *O'Brien*, C-432/17, EU:C:2018:879, paragraph 34).
- 134 Consequently, the temporal effects of a preliminary ruling given by the Court cannot depend on the date of delivery of the judgment by which the referring court rules finally on the main action, or even on the referring court's assessment of the need to preserve the legal effects of the national legislation at issue.
- 135 By virtue of the principle of primacy of EU law, rules of national law, even of a constitutional order, cannot be allowed to undermine the unity and effectiveness of EU law (see, to that effect, judgments of 26 February 2013, *Melloni*, C-399/11, EU:C:2013:107, paragraph 59, and of 29 July 2019, *Pelham and Others*, C-476/17, EU:C:2019:624, paragraph 78). Even assuming that overriding considerations of legal certainty are capable of leading, by way of exception, to a provisional suspension of the ousting effect which a directly applicable rule of EU law has on national law that is contrary thereto, the conditions of such a suspension can be determined solely by the Court (see, to that effect, judgment of 8 September 2010, *Winner Wetten*, C-409/06, EU:C:2010:503, paragraphs 61 and 67).
- 136 In this instance, since a risk of serious difficulties resulting from the interpretation adopted by the Court in the present judgment has not been shown to exist and the criteria referred to in paragraph 132 above are cumulative, it is not appropriate to limit the judgment's temporal effects.
- 137 In the light of the foregoing, the answer to the fourth question is that the principle of primacy of EU law must be interpreted as precluding the constitutional court of a Member State, before which a complaint has been brought challenging national legislation that proves, in the light of a preliminary ruling given by the Court of Justice, to be incompatible with EU law, from deciding, in accordance with the principle of legal certainty, that the legal effects of that legislation be maintained until the date of delivery of the judgment by which it rules finally on that constitutional complaint.

### Costs

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

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

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), must be interpreted as applying to the processing of personal data relating to penalty points imposed on drivers of vehicles for road traffic offences.**
2. **The provisions of Regulation (EU) 2016/679, in particular Article 5(1), Article 6(1)(e) and Article 10 thereof, must be interpreted as precluding national legislation which obliges the public body responsible for the register in which penalty points imposed on drivers of vehicles for road traffic offences are entered to make those data accessible to the public, without the person requesting access having to establish a specific interest in obtaining the data.**
3. **The provisions of Regulation (EU) 2016/679, in particular Article 5(1), Article 6(1)(e) and Article 10 thereof, must be interpreted as precluding national legislation which authorises the public body responsible for the register in which penalty points imposed on drivers of vehicles for road traffic offences are entered to disclose those data to economic operators for re-use.**
4. **The principle of primacy of EU law must be interpreted as precluding the constitutional court of a Member State, before which a complaint has been brought challenging national legislation that proves, in the light of a preliminary ruling given by the Court of Justice, to be incompatible with EU law, from deciding, in accordance with the principle of legal certainty, that the legal effects of that legislation be maintained until the date of delivery of the judgment by which it rules finally on that constitutional complaint.**

[Signatures]

---

\* Language of the case: Latvian.