



Reports of Cases

OPINION OF ADVOCATE GENERAL

BOBEK

delivered on 2 September 2021¹

Case C-175/20

SIA ‘SS’

v

Valsts ieņēmumu dienests

(Request for a preliminary ruling from the Administratīvā apgabaltiesa (Regional Administrative Court, Latvia))

(Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data and the free movement of such data – Legal basis for the processing – Obligation under national law for providers of Internet advertising services to provide, when requested by the tax authorities to do so, any information that they may have on taxable persons who have used those services – Requests for information addressed by the tax authority to the service provider – Scope – Material and temporal limits deriving from the GDPR)

I. Introduction

1. Regulation (EU) 2016/679 (‘the GDPR’)² is not a narrow piece of legislation. Its broadly defined scope of application, the effective judicial emptying of any exceptions to it,³ as well as the definitions-based, abstract and in consequence rather sweeping approach to its interpretation,⁴ have all contributed to making the reach of the GDPR virtually limitless. Indeed, if approached in this way, it is rather difficult nowadays to find a situation where someone is not processing some personal data somewhere at some stage.

2. That approach, grounded in the elevation of the protection of personal data under Article 8 of the Charter of Fundamental Rights of the European Union to an all-overriding fundamental (super-)right, nonetheless leads to distinct centripetal effects which the protection of personal data has started to exercise on other areas of law and disputes arising therein. A number of cases have started suddenly being portrayed as matters of personal-data protection and brought before

¹ Original language: English.

² 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).

³ Starting already, as regards the exceptions in Directive 95/46, with judgments of 20 May 2003, *Österreichischer Rundfunk and Others* (C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 41), and of 6 November 2003, *Lindqvist* (C-101/01, EU:C:2003:596, paragraphs 37 to 48). More recently, with regard to the GDPR, see judgment of 22 June 2021, *B (Penalty points)* (C-439/19, EU:C:2021:504, paragraphs 61 to 72).

⁴ See, for example, judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein* (C-210/16, EU:C:2018:388, paragraphs 29 to 39). However, see judgment of 29 July 2019, *Fashion ID* (C-40/17, EU:C:2019:629, paragraph 74).

(not only) this Court as a matter of interpretation of the GDPR. However, the specific issues raised in those disputes are, at times, not those expected to be governed by a piece of legislation such as the GDPR, despite its rather broad scope.

3. Indeed, few would have likely considered, beforehand, that the GDPR or its predecessor, Directive 95/46/EC,⁵ could be seen as governing the access of trainee accountants to their examination scripts, potentially coupled with the right of correction of those personal data after the examination has taken place;⁶ or as preventing the identification of an individual party to a traffic accident by the police so that the harmed party cannot sue in a civil court for reparation of damage done to the latter's vehicle;⁷ or as limiting the disclosure of information on previously paid tax by a bankrupt company to the insolvency administrator of that company in order to re-establish the equality between private law and public law creditors in the context of insolvency-avoidance claims,⁸ to name but a few of the more intriguing examples.

4. The present case is yet another example of such centripetal effects of the GDPR. SIA 'SS' is a provider of advertising services online. In the context of that commercial activity, it obtains the personal data of persons that place advertisements on its website. The competent national tax authority has asked that undertaking to forward to it a certain amount of data relating to second-hand car advertisements published on that website in order to ensure that the taxes on the sale of cars are properly collected. That tax authority has set out in detail the format of the data it wishes to receive. It has equally made clear that those data transfers are supposed to be permanent and apparently without financial compensation.

5. Against this background, the referring court enquires about the permissible scope of such data transfer requests. Like in previous cases, the GDPR appears to be applicable in the present case. Personal data is or will be processed somewhere by someone, certainly later on when executing the transfer. The rights of data subjects within such processing ought to be protected, just as the personal data involved should too. Nonetheless, that does not mean that the GDPR *specifically* regulates the relationship between a future controller (a public authority) and a present controller (a private undertaking). Indeed, the GDPR follows and protects the data wherever they go, thereby regulating the obligations of any successive controller vis-à-vis the data and towards the data subjects. Conversely, the GDPR does not regulate, except for a few explicit exceptions, the concrete details of the mutual relationship between two successive controllers of those data. In particular, the GDPR does not provide for the exact modalities of the arrangement between the controllers, whether it be of contractual or public law origins, under which one may request and obtain data from another.

⁵ 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).

⁶ Judgment of 20 December 2017, *Nowak* (C-434/16, EU:C:2017:994, paragraphs 18 to 23).

⁷ Judgment of 4 May 2017, *Rīgas satiksme* (C-13/16, EU:C:2017:336, paragraphs 12 to 17).

⁸ Judgment of 10 December 2020, *J & S Service* (C-620/19, EU:C:2020:1011, paragraphs 15 to 29).

II. Legal framework

A. EU law

6. Recital 31 of the GDPR reads as follows:

‘Public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission, such as tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. The requests for disclosure sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing.’

7. Recital 45 of the GDPR is worded as follows:

‘Where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.’

8. Article 2 sets out the material scope of the GDPR:

‘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;

...

(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. Article 4 contains definitions for the purposes of the GDPR:

‘(1) “personal data” means any information relating to an identified or identifiable natural person (“data subject”); ...

(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) “processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

(9) “recipient” means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

...’

10. Article 5 of the GDPR lays down the principles relating to the 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. Pursuant to Article 6 of the GDPR:

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

...

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

...

- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

...

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

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

- (a) Union law; or

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

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

12. Chapter III, entitled 'Rights of the data subject', sets out in Articles 12 to 22 the rights and corresponding obligations of controllers. Article 23 of the GDPR closes that chapter. It is entitled 'Restrictions' and provides that:

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

...

(e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;

...

2. In particular, any legislative measure referred to in paragraph 1 shall contain specific provisions at least, where relevant, as to:

- (a) the purposes of the processing or categories of processing;
- (b) the categories of personal data;
- (c) the scope of the restrictions introduced;
- (d) the safeguards to prevent abuse or unlawful access or transfer;
- (e) the specification of the controller or categories of controllers;
- (f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
- (g) the risks to the rights and freedoms of data subjects; and

- (h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.’

B. Latvian law

13. Under Article 15(6) of the Likums ‘Par nodokļiem un nodevām’ (‘Law on taxes and duties’), in the version in force at the time of the facts of the present case, providers of Internet advertising services have an obligation to provide, when requested to do so by the State Tax Administration, any information they may have on taxable persons who have used those services to publish advertisements and on the advertisements published by them.

III. Facts, national proceedings and the questions referred

14. On 28 August 2018, the director of the Nodokļu kontroles pārvalde (Tax Inspection Office) of the Valsts ieņēmumu dienests (Latvian Tax Authority) (‘the defendant’) sent SIA ‘SS’ (‘the applicant’) a request for information on the basis of Article 15(6) of the Law on taxes and duties.

15. In that request, the defendant urged the applicant to renew the former’s access to information on the telephone numbers of advertisers and the chassis numbers of vehicles featured in advertisements published on the applicant’s website (www.ss.com). The defendant also asked the applicant to provide, by 3 September 2018, information on advertisements published in the ‘Motor Vehicles’ section of the website during the period from 14 July to 31 August 2018. The applicant was asked to send the information electronically, in a format that would allow the data to be filtered and selected. The applicant was also asked to include the following information in the data file: a link to the advertisement, advertisement text, make of vehicle, model, chassis number, price, vendor’s telephone numbers.

16. In circumstances where it would not be possible to renew access, the applicant was asked to give the reason(s) why not and asked also to provide on a regular basis the information relating to the advertisements published no later than on the third day of each month.

17. The applicant lodged an administrative complaint challenging the request for information with the defendant’s acting director-general. According to the applicant, the scope of the request for information, which constitutes personal data within the meaning of Article 4(1) of the GDPR, was not justified by the law. The request does not specify a particular group of data subjects and does not indicate the purpose or scope of the scheduled processing or for how long the obligation to provide the information will last. As such, the defendant, in its capacity as controller, failed to act in accordance with the principle of proportionality or the principle of minimising the processing of personal data deriving from the GDPR to which the defendant is subject.

18. By decision of 30 October 2018 (‘the contested decision’), the defendant dismissed the complaint and upheld the request for information.

19. In the grounds of that decision, the defendant stated, in essence, that, in processing the abovementioned data, the tax authority performs the functions and exercises the powers conferred on it by law. The tax authority is responsible for collecting and auditing taxes, duties and other levies. It has a statutory duty to monitor the economic and financial activities of natural and legal persons in order to ensure that such dues are paid to the State and EU budgets.

In order to enable it to discharge those functions, the law confers on the defendant the power to gather the documents and information necessary to account for and record taxable events and to audit taxes and duties. In particular, under Article 15(6) of the Law on taxes and duties, providers of Internet advertising services are obliged to provide the tax authority, when requested to do so, with any information that they may have on taxable persons who have used those services to publish advertisements and on the advertisements themselves. Confidential information held by the defendant is protected by law, in particular by the prohibition on disclosure which is imposed on the tax authority's employees. It would follow that the request for information is lawful.

20. The applicant brought an action for annulment of the contested decision before the Administratīvā rajona tiesa (District Administrative Court, Latvia), claiming that the statement of grounds in that decision did not indicate the specific purpose of the data processing, nor the criteria for selecting the information requested in connection with a particular group of identifiable persons.

21. By judgment of 21 May 2019, the Administratīvā rajona tiesa (District Administrative Court) dismissed that action. In essence, it agreed with the defendant that no restriction could be placed on the amount of information to which the tax authority may have access in connection with any person, unless the information in question were considered to be inconsistent with the objectives of the administration of tax matters. According to that judgment, the information requested was necessary in order to identify undeclared economic activities. The provisions of the GDPR apply only to the applicant in its capacity as a service provider, not to the tax authority.

22. The applicant appealed that judgment before the Administratīvā apgabaltiesa (Regional Administrative Court, Latvia). According to the applicant, the GDPR is applicable to the case at hand. For the purposes of the personal data collected by means of the request for information, the defendant is to be regarded as the controller within the meaning of that regulation and must therefore comply with the requirements laid down therein. However, by issuing the request for information, the defendant has infringed the principle of proportionality by requiring every month a considerable amount of data relating to an undefined number of advertisements to be sent to it without indicating the specific taxable persons against whom the tax inspections have been initiated. The applicant states that the request for information does not indicate for how long the applicant will be subject to the obligation to provide the defendant with the information identified in that request. It thus takes the view that the defendant infringed the principles governing the processing of personal data, which are laid down in Article 5 of the GDPR (lawfulness, fairness and transparency). It contends that neither the request for information, nor the statement of grounds for the contested decision, specify the particular framework (purpose) within which the processing of the information prescribed by the defendant takes place, or the volume of information necessary (data minimisation). It submits that, in the request for information, the administrative authority must include clearly defined criteria for selecting the information required by that authority in connection with a particular group of identifiable persons.

23. In the referring court's view, it is not possible unequivocally to find that such a request for information is capable of being regarded as 'duly reasoned' and 'occasional' and that it does not relate to all of the information included in the 'Motor Vehicles' section of the applicant's website, given that the tax authority wishes, in essence, to carry out ongoing and exhaustive checks. The referring court harbours doubts as to whether the processing of personal data envisaged by the defendant can be regarded as compliant with the data-protection rules applicable in view of the purpose of the processing within the meaning of recital 31 of the GDPR. It is therefore necessary

to determine the criteria for assessing whether the defendant's request for information respects fundamental rights and freedoms and whether that request may be considered necessary and proportionate in a democratic society in order to safeguard important EU and Latvian public interest objectives in the taxation and budgetary fields.

24. According to the referring court, the request for information at issue does not make reference to any 'particular inquiry' carried out by the defendant within the meaning of the provisions of the GDPR. That request does not ask for information relating to specific persons, but rather relating to all data subjects who have published advertisements in the 'Motor Vehicles' section of the website. The tax authority also asks that that information be provided no later than on the third day of each month (meaning that the applicant must provide the defendant with all information on advertisements published in the previous month). In the light of the foregoing, the referring court wonders whether such a practice on the part of a national authority is compatible with the requirements laid down in the GDPR.

25. It is within this factual and legal context that the Administratīvā apgabaltiesa (Regional Administrative Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

- (1) Must the requirements laid down in the [GDPR] be interpreted as meaning that a request for information issued by a tax authority, such as the request at issue in this case, which seeks the disclosure of information containing a considerable amount of personal data, must comply with the requirements laid down in the [GDPR] (in particular Article 5(1) thereof)?
- (2) Must the requirements laid down in the [GDPR] be interpreted as meaning that the [Latvian] Tax Administration may depart from the provisions of Article 5(1) of that regulation even though the legislation in force in the Republic of Latvia does not empower it to do so?
- (3) For the purposes of interpreting the requirements laid down in the [GDPR], can there be considered to be a legitimate objective justifying the obligation, imposed by a request for information such as that at issue in this case, to provide all of the data requested in an undefined amount and for an undefined period of time, in the case where there is no prescribed expiry date for the fulfilment of that request for information?
- (4) For the purposes of interpreting the requirements laid down in the [GDPR], can there be considered to be a legitimate objective justifying the obligation, imposed by a request for information such as that at issue in this case, to provide all of the data requested even if the request for information does not (or does not fully) specify the purpose of disclosing that information?
- (5) For the purposes of interpreting the requirements laid down in the [GDPR], can there be considered to be a legitimate objective justifying the obligation, imposed by a request for information such as that at issue in this case, to provide all of the data requested even if that request relates in practice to absolutely all data subjects who have published advertisements in the "Motor Vehicles" section of a portal?
- (6) What criteria must be used to verify that a tax authority, acting as controller, is duly ensuring that the processing of data (including the collection of information) is compliant with the requirements laid down in the [GDPR]?

- (7) What criteria must be used to verify that a request for information such as that at issue in this case is duly reasoned and occasional?
- (8) What criteria must be used to verify that personal data are being processed to the extent necessary and in a manner compatible with the requirements laid down in the [GDPR]?
- (9) What criteria must be used to verify that a tax authority, acting as controller, ensures that data are processed in accordance with the requirements laid down in Article 5(1) of the [GDPR] (accountability)?

26. Written observations have been submitted by the Belgian, Greek, Spanish and Latvian Governments, as well as the European Commission. The applicant, the Belgian, Spanish and Latvian Governments, together with the Commission, responded to written questions put by the Court in accordance with Article 61(1) of the Rules of Procedure of the Court of Justice.

IV. Assessment

27. This Opinion is structured as follows. I shall start by addressing whether the GDPR is applicable to a request from a public authority to a controller for the transfer of a certain amount of personal data. In view of the questions raised by the referring court, a twofold clarification at the outset is necessary: who exactly is who in the main proceedings and what specific rules does the GDPR provide in such cases (A). Next, I shall turn to the (rather basic) legal framework that derives from the GDPR vis-à-vis requests for data transfers addressed by public authorities to private undertakings (B). I shall then conclude with several remarks on what constitutes, at least in my view, the actual thorny issue of this case, even though it has not expressly been raised by the referring court (C).

A. *The applicability of the GDPR*

28. The referring court has raised nine questions, each concerning, in one way or another, the lawfulness of specific request(s) for the transfer of certain personal data from private undertaking(s) issued by a tax authority for the purposes of tax collection and tax evasion detection. The personal data at issue have been obtained by the private undertaking in the framework of its regular business activity from data subjects.

29. Nevertheless, it is not obvious from the nine questions raised *who* precisely is under *what obligation*, and on the basis of *which provision* of the GDPR. That ambiguity is rather indicative of a significant degree of uncertainty as regards the framing of this case in at least two ways.

30. First, within the categories established by the GDPR, *who is who* in this case? The case is concerned with the transfer, from the private undertaking to the public authority, of certain data from a larger data set collected and controlled by the private undertaking. That is the specific processing operation within the meaning of Article 4(2) of the GDPR that forms the basis of the questions before this Court.

31. However, it also appears that, with regard to that transfer of data, the referring court considers the tax authority (the defendant) to be the controller for that specific processing operation already.⁹ That assumption, which underpins the entire order for reference, is expressly articulated in Questions 6 and 9. That requires a preliminary clarification: *who* exactly is to comply with the GDPR in the present case? Who is the controller for that specific processing operation? (2)

32. Second, due to that uncertainty there is another important issue: *what* are the specific GDPR *provisions* that apply to requests for data transfers, and which of those provisions relate, in particular, to the type and quantity of data that a public authority might require from a private undertaking? It is quite revealing in this regard that three of the referring court's questions only mention Article 5(1) of the GDPR, a transversal provision setting out the principles relating to the processing of personal data by any controller. By contrast, the other questions refer simply to the 'requirements laid down in the GDPR' without specifying which specific provisions ought to contain those requirements.

33. Thus, another preliminary clarification is called for in relation to the applicable provision(s) of the GDPR, in particular as regards the relationship between the applicant undertaking and the defendant tax authority. How does the GDPR specifically regulate such data transfer requests and the mutual rights and obligations between a private undertaking and a public authority? (3)

34. That said, before addressing those two issues, I shall recall why, in my view, the application of and the compliance with the GDPR cannot be viewed in an abstract manner, interpreting definitions that do not relate to a specific processing operation that ought to be taken as a point of departure. Once that has been explained, only then is it possible correctly to analyse the actors and their respective obligations (1).

1. The abstract definitions and the all-embracing GDPR

35. In the present case, all interested parties, including the Latvian Government, agree that, if the starting point of the analysis is based on the legislative definitions of 'personal data' and 'processing' laid down in Article 4 of the GDPR, then that instrument is certainly applicable to the case in the main proceedings.

36. First, the data concerned by the request for information are *personal data* within the meaning Article 4(1) of the GDPR. The information requested, such as the phone number of data subjects or the car chassis number, constitute 'information relating to an identified or identifiable person'. Indeed, that information allows car sellers and, therefore, potential taxpayers to be identified.

⁹ Contrary to what seemed to be the position of the first-instance court, the Administratīvā rajona tiesa (District Administrative Court), which took the view that for this stage of the data-processing the controller was the applicant (see above, point 21 of this Opinion).

37. Second, it is established case-law that the communication of data¹⁰ or the disclosure of personal data by transmission, like the storage or otherwise making available of data, constitute *processing*.¹¹ After all, ‘disclosure by transmission’ is included in the descriptive list of processing operations under Article 4(2) of the GDPR.

38. Third, that processing of personal data is clearly carried out by automated means within the meaning of Article 2(1) of the GDPR.

39. Furthermore, none of the exceptions, which must in any event be interpreted narrowly,¹² is applicable in the present case. In the light of *Österreichischer Rundfunk and Others*,¹³ and in particular following the recent *Penalty Points* case,¹⁴ it cannot be argued that the processing of personal data at issue has taken place ‘in the course of an activity which falls outside the scope of Union law’ within the meaning of Article 2(2)(a) of the GDPR.

40. Equally, the exception laid down in Article 2(2)(d) of the GDPR does not appear to be triggered either. ‘Competent authorities’ under that provision appear to be bodies such as the police or the State prosecutorial services.¹⁵ They do not include tax authorities acting for tax collection purposes, nor, and even less so, Internet services advertising providers. Furthermore, even if data processing by the competent tax authorities might in some cases eventually result in the detection of a criminal offence in the form of a tax fraud, that is merely a hypothetical possibility at this stage.¹⁶

41. Thus, if approached in this way, one is bound to conclude that the GDPR does apply: there is personal data which is being processed by automated means. However, as already alluded to in the introduction to this Opinion, such an approach, based on the relevant concepts under Article 4 of

¹⁰ See, for example, judgments of 29 June 2010, *Commission v Bavarian Lager* (C-28/08 P, EU:C:2010:378, paragraph 69), and of 19 April 2012, *Bonnier Audio and Others* (C-461/10, EU:C:2012:219, paragraph 52).

¹¹ See, for example, judgments of 29 January 2008, *Promusicae* (C-275/06, EU:C:2008:54, paragraph 45), and of 6 October 2020, *Privacy International* (C-623/17, EU:C:2020:790, paragraph 41), in the context 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 also judgment of 6 October 2015, *Schrems* (C-362/14, EU:C:2015:650, paragraph 45), in the context of transfers of data to a third country.

¹² See, for example, judgment of 9 July 2020, *Land Hessen* (C-272/19, EU:C:2020:535, paragraph 68).

¹³ Judgment of 20 May 2003, *Österreichischer Rundfunk and Others* (C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraph 39 to 47).

¹⁴ Judgment of 22 June 2021, *B (Penalty points)* (C-439/19, EU:C:2021:504, paragraphs 61 to 72).

¹⁵ See, to that effect, Article 3(7) of 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).

¹⁶ With that hypothetical future possibility hardly being conclusive for defining *ex ante* the normative scope of applicability of an EU law instrument. See also my Opinion in Joined Cases *Ministerul Public – Parchetul de pe lângă Înalta Curte de Casație și Justiție – Direcția Națională Anticorupție and Others* (C-357/19 and C-547/19, EU:C:2021:170, points 109 to 115), regarding a similar argument with regard to the scope of application of Article 325(1) TFEU.

the GDPR, such as ‘processing’,¹⁷ ‘personal data’¹⁸ or ‘controller’,¹⁹ being interpreted extensively and outside of any specific processing operation, means that *any* communication of *any* information would be governed by the GDPR.

42. In order to interpret correctly the obligations of all actors involved, the starting point of an analysis under the GDPR should be the clear identification of a *specific processing operation*. Only then can one properly proceed to the assessment of the obligations arising under the GDPR for that specific operation for the actual actors involved in that processing.²⁰ It is the specific processing operation, the work on and with the data, that is being regulated. The regulatory logic and focus of the GDPR is performance-based and process-oriented, and thus necessarily dynamic.

2. Who is who in the present case?

43. What is the specific processing operation in the present case? The execution of requests for information such as those in the main proceedings undoubtedly require the processing of personal data to which the GDPR will be in principle applicable. In the present case, there are two different entities which carry out data processing at some stage. In its questions, the referring court focuses on processing *by the defendant*, that is, the national tax authority. However, from the facts of the case, it would appear that processing *by the applicant*, that is, the private undertaking, would have to be carried out first.

44. In the judgment in *Fashion ID*,²¹ the Court looked at the *specific operations* at issue within the processing of data in order to identify the relevant controller(s). The Court found that the concept of ‘controller’ does not necessarily refer to a single entity and may concern several actors taking part in that processing, with each of them then being subject to the applicable data-protection provisions.²² However, a natural or legal person cannot be considered to be a controller in the context of *operations that precede or are subsequent* in the overall chain of processing for which that person does not determine either the purposes or the means.²³

45. In the present case, the defendant is likely to be the controller *once* it has received the requested data from the applicant and begins processing them within the meaning of Article 4(2) of the GDPR.²⁴ At that stage, the defendant will not only start processing the data, but is also likely to define the means and purposes of its own processing for the purposes of Article 4(7) of the GDPR. When carrying out *itself* any future data processing operations, the defendant will *then* have to comply – provided that no restrictions under Article 23 of the GDPR have been adopted

¹⁷ See, for example, to that effect, judgments of 11 December 2014, *Ryneš* (C-212/13, EU:C:2014:2428, paragraphs 30), and of 10 July 2018, *Jehovan todistajat* (C-25/17, EU:C:2018:551, paragraph 51). In the latter case, the Court held that the collection of personal data by members of a religious community in the course of door-to-door preaching and the subsequent processing of those data may fall within the material scope of the GDPR.

¹⁸ See, for example, judgment of 20 December 2017, *Nowak* (C-434/16, EU:C:2017:994, paragraph 62), where the Court held that the written answers submitted by a candidate at a professional examination and any comments made by an examiner with respect to those answers constituted personal data.

¹⁹ See, for example, judgments of 13 May 2014, *Google Spain and Google* (C-131/12, EU:C:2014:317, paragraph 34), and of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein* (C-210/16, EU:C:2018:388, paragraphs 28 to 44), where the Court held that the concept of ‘controller’ encompasses the administrator of a fan page hosted on a social network.

²⁰ See judgment of 29 July 2019, *Fashion ID* (C-40/17, EU:C:2019:629, paragraphs 72 and 74).

²¹ Judgment of 29 July 2019, *Fashion ID* (C-40/17, EU:C:2019:629).

²² *Ibid.*, paragraph 67.

²³ *Ibid.*, paragraph 74.

²⁴ For a recent illustration of processing by public authorities, see judgment of 9 July 2020, *Land Hessen* (C-272/19, EU:C:2020:535, paragraphs 64 and 65).

by the Member State in this regard – with the principles relating to data quality laid down in Article 5 of the GDPR, and with grounding its processing operation(s) in one of the scenarios under Article 6(1) of the GDPR.²⁵

46. However, it is apparent from the order for reference that the present proceedings have not yet reached that stage. The tax authority is not in possession of the requested data. Therefore, it could not have begun any processing operation of those data. Furthermore, the Court has received no information on what the defendant intends to do with the data or the kind of processing that would be carried out on its part.

47. All that has happened *so far* is that the tax authority has requested a private undertaking to provide it with a given data set. That, in itself, is not processing of any personal data, certainly not of the data that has yet to be obtained. Within such a factual scenario, the applicant, the private undertaking, remains the controller of the data in as much as it has obtained the data in the first place by way of its own activity, thus for self-defined means and purposes. While processing the data in its possession in order to communicate those data to the defendant according to the conditions it received, the applicant remains the controller for that processing operation as well. It is the applicant that carries out such further processing.²⁶

48. In that context, and in accordance with Article 6(1)(c) of the GDPR, the applicant thereby ensures compliance with a legal obligation to which it is subject as a controller, namely with Article 15(6) of the Law on taxes and duties. In its capacity as controller, the applicant is also required to comply with the GDPR when processing personal data, as well as for the communication of those data to the defendant. However, the referring court is not enquiring about the scope of the *data processing* required from the applicant to execute the request at issue. In fact, it has not asked any questions regarding possible GDPR-based obligations *of the applicant* when carrying out that processing.

49. By singling out the *defendant* as the presumed bearer of obligations under the GDPR, the referring court appears to be concerned with the (legal) *basis for the processing* within the meaning of Article 6(3) of the GDPR, that is to say, with Article 15(6) of the Law on taxes and duties, as further implemented by requests for information filed by the defendant.

50. In summary, the key issue underpinning all nine of the referring court's questions appears to be that of the scope and conditions of personal-data transfers between two successive controllers.²⁷ What are the provisions of the GDPR, if any, that govern the relationship between successive controllers? Does the GDPR contain any (material or temporal) limits to the scope and type of transfers of personal data between two controllers, in the present case a private undertaking and a public authority? All those issues properly pertain to the *legal basis* for obtaining personal data, and do not really concern the processing operation.

²⁵ See, for example, judgment of 16 January 2019, *Deutsche Post* (C-496/17, EU:C:2019:26, paragraph 57). See also, to that effect, judgments of 1 October 2015, *Bara and Others* (C-201/14, EU:C:2015:638, paragraph 30), and of 27 September 2017, *Puškár* (C-73/16, EU:C:2017:725, paragraph 104).

²⁶ As notably provided for in Article 13(2) of the GDPR, albeit in another context, namely that of the information to be provided.

²⁷ For the sake of completeness, it might be added that other scenarios foreseen under the GDPR, such as *joint control* between the tax authority and the private undertaking over that given stage of processing (Article 26), or the relationship of a somewhat construed *de facto controller and processor* (Article 28), appear to be excluded on the facts as presented by the referring court.

3. *Specific obligations flowing from the GDPR?*

51. The GDPR is primarily concerned with the protection of personal data of data subjects and the relationship between those subjects and any entity processing their data. To that effect, the GDPR lays down the rights of the data subjects and the obligations of the relevant controllers within the processing of personal data.

52. Such a regulatory logic focuses on the data and the entities accessing them and working with them. There are very few provisions in the GDPR that directly and expressly regulate the relationship between the data processing entities.²⁸ It is true that the GDPR reaches into those relationships indirectly. It obliges any subsequent entity that obtains the data to protect the data and the rights of the data subjects. In such a manner, the GDPR indeed sets certain conditions for data disclosure and data transfers. However, that certainly does not mean that the GDPR would directly regulate the relationships between those entities.

53. In a way, if data were to be seen as goods, then the regulatory logic of the GDPR is analogical to a specific public law regime for certain types of (precious, artistic, historical) goods. Such a regime imposes certain limitations on those goods: how such goods can be manufactured, how they are to be used, under what conditions they can be altered, stored, resold, or destroyed. Such a specific regime protects the goods and thereby indirectly binds any successive owner or possessor of those goods. However, in and of itself, that specific regime remains tied to the goods. It does not regulate either the private arrangements under which such goods might be sold between two private parties, or the conditions under which the same goods might or must be passed on from a private entity to a public one. Regulating the goods is different from regulating the underlining legal title to and trade in those goods.

54. It is only by clarifying that regulatory logic of the GDPR, as well as focusing on the specific processing operation as the starting point for the potential obligations arising under that instrument, that the GDPR can reasonably be interpreted. Otherwise, the GDPR will always be applicable, while, on however creative reading of it, there will simply be no provision that would govern the specific question submitted. The inevitable result of such cases will be that the GDPR is not opposed to certain national legislation or practice. Yet, that ‘absence of opposition’ will not necessarily be the result of the national regimes being in general lawful, but rather that such an issue is simply not regulated by the GDPR, even if it touches, in one way or another, on personal data.

55. The Court’s case-law is familiar with such ‘false positives’ as regards diverse obligations to disclose data provided for under national law for different reasons. Again, most of such cases do not concern any ongoing processing operation as such, but rather the upstream issue of the legal basis for such a future operation. They range from the initiation of civil proceedings to enforce

²⁸ With the two notable exceptions in Articles 26 and 28 of the GDPR mentioned in the previous footnote, or, for instance, Article 19 of the GDPR. However, also with regard to those provisions, the regulatory inclusion of these categories could still be considered as one of data protection, essentially ensuring that the controller cannot abdicate responsibility and escape liability either by sharing the data, or by outsourcing its processing.

copyrights,²⁹ to the proper management of public funds,³⁰ or the safeguarding of national security.³¹ Examples under this heading might also include cases such as *Rigas satiksme*,³² *Promusicae*,³³ *Bonnier*,³⁴ or *J & S Service*.³⁵

56. Certainly, in all those situations, the GDPR was applicable with regard to the rights of the data subjects vis-à-vis the controller(s) in the context of specific processing operations that had just happened or were about to happen. However, and yet again, the regulatory logic and the proper scope of the GDPR must follow the data flow and ensure that personal data are protected within processing operations. It is not meant to regulate any and every upstream relationship between various entities that might be in possession of data, including the reasons why and how they might come into the possession of those data. In other words, the GDPR does not guarantee any ‘rights’ of one controller against another controller.

57. This is not to say that such issues are not regulated by law. They are, but by other instruments concerned primarily with law enforcement. It is in those instruments that one finds the legal basis for the processing that is required by Article 6(3) of the GDPR in the first place. When it comes to *compulsory* transfers of personal data, those transfers tend to be indeed, rather logically, provided for in ‘law enforcement instruments’, be it under EU law³⁶ or national law. When it comes to *voluntary* transfers of personal data, as far as is possible and permitted by the public law regime that is the GDPR, the basis for those transfers will be national business law or contract law, in view of the type of arrangements in place between the respective successive controllers.

58. Taking these clarifications into account, in my view, this case is not (yet) about any processing operation. It is about the legal basis for that processing, which is a matter to which the GDPR only refers, but does not itself directly regulate. However, that being said, and in an effort fully to assist the referring court, what follows in the subsequent section of this Opinion is the outline of the basic framework that derives from the GDPR and that will be applicable to the processing operation once carried out by the controller, the private undertaking (B). The aim of the GDPR is to protect the data subject, not a private undertaking against a public interference with its freedom to conduct a business or its right to property in the form of data exploitation. This is not to suggest that such an issue cannot give rise to a valid concern, but rather that it can hardly be regulated by the GDPR (C).

²⁹ See, for example, judgments of 24 November 2011, *Scarlet Extended* (C-70/10, EU:C:2011:771).

³⁰ Judgment of 20 May 2003, *Österreichischer Rundfunk and Others* (C-465/00, C-138/01 and C-139/01, EU:C:2003:294).

³¹ See, for example, judgments of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970), and of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791).

³² Judgment of 4 May 2017, *Rigas satiksme* (C-13/16, EU:C:2017:336).

³³ Judgment of 29 January 2008, *Promusicae* (C-275/06, EU:C:2008:54).

³⁴ Judgment of 19 April 2012, *Bonnier Audio and Others* (C-461/10, EU:C:2012:219).

³⁵ Judgment of 10 December 2020, *J & S Service* (C-620/19, EU:C:2020:1011).

³⁶ See, for example, under EU law, Article 4 of former Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54), or Article 8 of Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ 2016 L 119, p. 132).

B. (Legal basis for) personal-data transfers to public authorities

59. What follows is a rather general discussion concerning the *legal basis* for the data processing that the applicant would have to carry out when executing the defendant's request for information. In that regard, the relevant provision is likely to be Article 6 of the GDPR, and in particular paragraphs 1 and 3 thereof, read in the light of recital 45.

60. As a preliminary point, it is worth mentioning the fact that no specific information has been provided to this Court concerning any additional applicable national rules on data protection in circumstances such as those in the main proceedings. Moreover, the Court has also not received any information on whether there are, beyond Article 15(6) of the Law on taxes and duties, other national acts of general application (for example, a decree or implementing guidelines) that would further regulate the obligation at issue for (Internet advertising) service providers to communicate certain data to tax authorities. There is also very little information on the national legislative framework implementing the GDPR in general.

61. Furthermore, it has not been made clear whether Article 23(1)(e) of the GDPR has been implemented into national law in any way. Whether that EU law provision has or has not been implemented does not determine the legality of the request for the transfer of information. However, it would be relevant for determining the scope and nature of the obligations that a subsequent controller (a public authority) might have vis-à-vis the data subjects, as well as for determining the obligations of the original controller and the information that the latter shall provide to the data subjects.

62. As a result, the following discussion cannot be but a somewhat general one. I shall address the principles flowing from Article 6 of the GDPR for the future processing to be carried out by a private undertaking in order to comply with a data request from a public authority, first in terms of the purpose of such data transfers (1) and their scope and duration (2). I shall then turn to the legal basis of such transfers since the requirements regarding that basis become clearer once the previous sub-issues have been addressed (3).

1. Purpose

63. In general, the overall purpose for which the tax authority seeks the disclosure of personal data in the main proceedings is without doubt legitimate. Ensuring the proper collection of tax and detecting potential breaches of the duty to pay tax can certainly fall under the types of legitimate aims and purposes for data processing pursuant to both Articles 6(1) and (3) of the GDPR.³⁷

64. The key to the issues raised by the present case is the level of abstraction at which such an aim should be stated. In that regard, there appears to be a degree of confusion between two types of specific aims: (i) *searching* for certain types of information (in order to detect breaches of the law), as opposed to (ii) *verifying* the fact that certain infringements have occurred (and seeking the disclosure of specific data in order to confirm that assumption).

³⁷ See, for example, to that effect, judgment of 27 September 2017, *Puškar* (C-73/16, EU:C:2017:725, paragraph 108), as regards the establishment of a list by a public authority for the purposes of collecting tax and combating fraud.

65. The nature (and accordingly the scope) of both types of data disclosure transfers is bound to differ. The logic of *searching and detecting* is *ex ante*, broad, and largely indeterminate as to the exact data subjects. If the aim is to detect possible breaches, then the metaphorical net is to be cast rather wide. By contrast, the logic of *verifying* potential breaches through the disclosure of relevant data can be much more nuanced and focused. There, the logic is far more *ex post*, focused on verifying certain suspicions typically relating to an already discernible data subject.

66. In my view, Article 6 of the GDPR permits both scenarios. That said, Article 6(3) of the GDPR requires a clear legal basis for either of those data transfers.

67. However, I understand the hesitations of the referring court in the context of the present case, when taking into account the wording of Article 15(6) of the Law on taxes and duties. In the wording that was apparently in force when the referring court submitted its request for a preliminary ruling, it stated that the providers of Internet advertising services might be obliged, upon a request made by the State Tax Administration, to provide information on the (respective) tax persons.

68. It would therefore appear that, in the present case, the purpose of the disclosure, stated in the relevant legal basis, resembles the second scenario outlined above: verifying certain information with regard to specific tax persons. However, the national tax authority seems to have used that legal basis for what appears to be a request for (unlimited) data transfers or even outright data harvesting, in order to carry out a general search and detection exercise, falling within the first scenario outlined above. It is here that one finds the logical dissonance that appears to lie at the bottom of this case at the national level, resulting in a sense of confusion about both the proportionality of such a measure (2) and its proper legal basis (3).

2. *Scope and duration*

69. Proportionality, as well as ‘minimisation’ for that matter, is an examination of the relationship between the (stated) aims and the (chosen) means. The problem in the present case is that, depending on which of the aims is chosen from amongst the two (ideal³⁸) scenarios just outlined, the assessment of proportionality is likely to differ.

70. Within the framework of a ‘search and detect’ objective, public authorities will cast their net as wide as they can in order to ensure that relevant information can be found. That may entail the processing of a large quantity of data. Indeed, the need to obtain and process larger data sets is inherent in that type of general and indeterminate information search. In that scenario, the proportionality and the minimisation of data processing can only really relate to the *type* of data requested where the necessary information can potentially be found.³⁹

71. Within the framework of a ‘verification’ objective, where the public authorities need to obtain evidence relating to the content of a specific transaction or set of transactions, the proportionality assessment can naturally be more demanding. The tax authority may then only ask for specific

³⁸ Ideal in the sense that the two outlined scenarios represent two extremes on an imaginary line, rather than hermeneutically sealed boxes.

³⁹ Yet again underlining the true nature of this case, which is much closer to the scenarios in which the Court was called upon to examine various scenarios of data retention or data transfers to third countries than a ‘true’ GDPR case (see above in points 56 and 57 of this Opinion, as well as the case-law quoted in footnotes 11, 31, and 44).

transactions, within a specific time frame, in order to make *ex post* verifications, typically with regard to the given taxable person(s). Requests for information are likely therefore to be tailored to the *specific* data that contain that type of information.

72. The logic of recital 31 of the GDPR, to the extent that I am able to discern any, seems to pertain to the latter scenario only. The second sentence of that recital, which has been relied on and abundantly discussed by the interested parties, in particular the Commission, states that the requests for data communication sent by the public authorities should always be in writing, reasoned and occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems.

73. However, in my view, it is not possible to take (part of) a recital in a regulation out of its context, treat it as an independent and binding provision, without it even being echoed somewhere else in the legally binding text of that instrument,⁴⁰ and on that basis proclaim that any transfers of personal data to public authorities may occur under those conditions only. I simply cannot embrace the suggestion that a part of recital 31, taken in isolation, bans all larger scale data transfers to public authorities, even those that have an appropriate legal basis (in national and/or EU law) and are compliant with all binding provisions of the GDPR.

74. In the context of the present case, the Latvian Government maintained that the amount of information requested can be considered reasonable in so far as the request for communication only includes advertisements published in the ‘Motor Vehicles’ section, which is 1 section out of 112 sections of the concerned website run by the applicant. The Belgian and Spanish Governments have added that, in their view, the issue is not the amount of data but rather the type of data requested.

75. I agree with those observations.

76. Proportionality for *ex ante* search and detection means a ‘quality check’ with regard to the type of data requested. It is only for *ex post* verification of certain facts that the ‘quantity check’ can be fully deployed. Were it to be otherwise, most means of data monitoring or surveillance would be, in practice, excluded.

77. Provided that there is an appropriate legal basis in EU or national law, a national tax authority may in principle request all the necessary data for the type of examination it needs to carry out, without any temporal limitation. The only limit flowing from the GDPR is the proportionality in terms of the type of data requested. As the Greek Government correctly points out, requests for information should be limited to the type of data concerning the economic activity of taxpayers, as opposed to their private life.

78. To provide an example, if the stated purpose is to detect non-declared incomes from the sale of second-hand cars, the tax authority does not have the right also to request information on whether or not the person selling the car is a redhead, whether he or she follows a particular diet, or whether he or she owns a swimming pool. Therefore, the type of information requested must clearly relate to the search and investigation disclosed.

⁴⁰ See, for example, judgment of 12 July 2005, *Alliance for Natural Health and Others* (C-154/04 and C-155/04, EU:C:2005:449, paragraphs 91 and 92); of 21 December 2011, *Ziolkowski and Szeja* (C-424/10 and C-425/10, EU:C:2011:866, paragraphs 42 and 43); or of 25 July 2018, *Confédération paysanne and Others* (C-528/16, EU:C:2018:583, paragraphs 44 to 46 and 51).

79. Other than that, the assessment of proportionality in either of the two scenarios set out above is for the national court to carry out in the light of the factual and legal circumstances of each case.⁴¹ Put simply, in the present case, the question one must ask is whether the type of data requested is suitable in order for the defendant to obtain the necessary information to carry out its stated aim.

3. *Legal basis (for the future processing)*

80. Finally, it is only now that the key issue of the legal basis can be usefully assessed in view of the clarifications just made. Naturally, both scenarios outlined in the previous subsections of this Opinion ('search and detect' and 'verification') require a legal basis under Article 6(3) of the GDPR in order for the processing by the applicant to take place. That provision expressly allows for specific adaptation of the application of the general rules of the GDPR, be it by EU law or the law of the Member States.

81. In any event, however, the legal basis provided for must logically cover the specific purpose and type of processing carried out for that purpose. How exactly it will go about that is a matter of specific adaptation provisions adopted by the Member State or the Union under Article 6(3) of the GDPR. In general, the more generalised, larger and permanent the data transfers, the more robust, detailed and express the *legislative* basis must be since such data transfers represent a greater interference with the safeguarding of data protection. By contrast, the more discreet and limited the disclosure requests – usually with regard to one or a few data subjects only, or even with regard to a limited amount of data – the more likely those requests can be carried out at the level of individual *administrative* requests, with the legislative empowering clause remaining rather broad and generic.

82. In other words, the two regulatory layers, namely the legislative and the administrative, making up the eventual legal basis for the data processing, operate jointly. At least one of them must be sufficiently specific and tailored to a certain type or a certain amount of personal data requested. The more there is at the legislative, structural level for such data transfers, the less there needs to be in the individual administrative request. The legislative layer might even be so detailed and comprehensive that it will be completely self-contained and self-executing. By contrast, the more generic and vague the legislative level, the more detail, including a clear statement of purpose which will thus delimit the scope, there will need to be at the level of the individual administrative request.

83. This point indirectly provides an answer to the issue raised by the referring court under the heading of proportionality, which might in fact best be addressed here in determining whether tax authorities can make requests for data that are unlimited in time. In my view, under the GDPR, they can. However, the more pertinent question ought to be whether they have an appropriate legal basis in national law for what is, as to its substance, an ongoing and permanent data transfer. So long as such transfers have a clear basis, as well as duration, in national law, Article 6(3) of the GDPR does not preclude them. Again, recital 31 of the GDPR changes little in that regard.⁴² I see little practical sense in reading that recital as effectively requiring the administrative authorities to issue time and again (whether it be each day, month, or year) identical individual requests in order to obtain something that they could have already obtained on the basis of national legislation.

⁴¹ See also, to that effect, judgment of 27 September 2017, *Puškar* (C-73/16, EU:C:2017:725, paragraph 113).

⁴² See already above, points 72 to 73 of this Opinion.

84. In the present case, the legal basis for the processing appears to be constituted by both Article 15(6) of the Law on taxes and duties and the specific requests for the disclosure of data made by the tax authority. There thus appears to be a two-fold legal basis with a general legislative empowerment clause and its specific, targeted administrative application of that provision.

85. On the whole, such a dual legal basis appears to be sufficient to justify the processing of personal data by the applicant for the purposes of its transfer to a public authority under Article 6(1)(c) and (3) of the GDPR. Although the national legislation empowering tax authorities to request information remains rather general, the specific requests for data appear largely to target a certain type of data despite its potentially large amount.

86. However, it is ultimately for the national court to verify, in full knowledge of national law, including any further national implementing rules not mentioned in the course of the present proceedings, whether or not the requested processing by the applicant in the main proceedings meets the requirements set out in the present section of this Opinion.

87. The issue that lies at the heart of that assessment, which requires particular attention, is whether Article 15(6) of the Law on taxes and duties, together with the specific requests for information, complies with the requirement of foreseeability⁴³ when examining the legal basis. The legislation allowing for data transfers must lay down clear and precise rules governing the scope and application of the measure in question and impose minimum safeguards, so that the persons whose personal data is affected have sufficient guarantees that those data will be effectively protected against the risk of abuse.⁴⁴

88. Therefore, the legal basis taken as a whole (legislative and administrative combined) must be formulated with sufficient precision for all the persons concerned: the public authorities as regards what they may ask, the undertakings in relation to what they may provide and, above all, the data subjects so that they know who might have access to their data and for what purposes. It might be recalled that information about data processing is indeed a key requirement under the GDPR. The data subjects must be aware of the existence of such processing and that information is the prerequisite to exercise further rights to access or to erasure or rectification.⁴⁵

89. Unless Article 23 of the GDPR has been in any way transposed into national law in order to restrict the rights of data subjects under Chapter III of the GDPR, it follows from Articles 13 and 14 of the GDPR that the controller of the processing is to provide the data subject with information. In the context of successive data transfers, it might be difficult to determine on whom the duty of information is incumbent.⁴⁶ Moreover, in practical terms, absent any restrictions adopted under Article 23(1) of the GDPR, which in national law must meet the requirement of Article 23(2) of the GDPR, a public authority who obtained the data might be under an obligation to provide the appropriate information under Article 14 of the GDPR to all the data subjects concerned. If there is no clear and foreseeable legal basis which permits such data transfers ultimately to take place, it can hardly be expected from the controller who collected the data to inform already the data subject accordingly under Article 13 of the GDPR.

⁴³ See, for example, to that effect, judgment of 20 May 2003, *Österreichischer Rundfunk and Others* (C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraphs 77 and 79).

⁴⁴ See, for example, more recently, judgment of 6 October 2020, *Privacy International* (C-623/17, EU:C:2020:790, paragraph 68).

⁴⁵ See, to that effect, judgment of 1 October 2015, *Bara and Others* (C-201/14, EU:C:2015:638, paragraph 33).

⁴⁶ See, to that effect, judgments of 1 October 2015, *Bara and Others* (C-201/14, EU:C:2015:638, paragraph 34 to 38), and of 16 January 2019, *Deutsche Post* (C-496/17, EU:C:2019:26, paragraph 69).

90. In conclusion therefore, in my view, Article 6(1)(c) and (3) of the GDPR does not preclude national rules from laying down, without any limit in time, an obligation for Internet advertising service providers to communicate certain personal data to a tax authority, as long as there is a clear legal basis in national law for such a type of data transfer and the data requested are suitable and necessary for the tax authority to complete its official tasks.

C. A coda: the question that was not raised in the present case

91. It is hardly my role to speculate about genuine motives of the parties before the national court. I shall therefore stay true to my hope in the existence of Good Samaritans, who selflessly step up in defence of others. Why is it that a private company could not simply be defending the rights of the data subjects from whom they collected their personal data?

92. Although one can all but rejoice when commercial undertakings become committed to the cause of data protection, I assume that some other undertakings may also have other reasons why they might wish to oppose public-power-decreed transfers of personal data they collected. One reason might relate to the costs of such an endeavour. Should the public authorities be allowed effectively to outsource part of the exercise of public administration, forcing the private undertakings to bear the costs for the exercise of what essentially is public administration? That issue becomes significant in cases of permanent, large-scale data transfers that are supposed to be carried out by private undertakings for the common good without any compensation.⁴⁷ Other reasons might be more business-related. If one assumes for a fleeting moment, naturally at the level of pure hypothesis, that people in general do not enjoy paying taxes, it may not be far-fetched also to assume that some of those people might choose different avenues for the advertising of their second-hand cars than a website which later communicates that information to the tax authorities.

93. Finding an equilibrium between all the interests present in such a situation is far from straightforward. On the one hand, for the public power to request data from private undertakings, which must be prepared and submitted according to the former's exact requirements, could come dangerously close to forced outsourcing of the exercise of public administration. That might be particularly the case with regard to the data that are otherwise freely available and which the public bodies could have collected themselves with a little technical effort. On the other hand, as the Belgian Government pertinently emphasised by pointing out the broader relevance of the situation in the main proceedings, a slightly more nuanced answer might perhaps be called for in the situations of various forms of shared-economy platforms, or in other scenarios whereby the public authorities request access to data which are essential for the stated legitimate public purpose, but which are not freely available, thus not capable of being collected by the public authorities themselves. However, even in such circumstances, the issue of possible compensation remains open.

94. I certainly see such issues lurking in the background of the main proceedings. However, finding a reasonable balance for such cases should primarily take place at the national or EU level when adopting the relevant legislation providing the legal basis for such a type of transfer. It should not be a matter of judicial intervention, a fortiori in a case in which the referring court did not even raise any of those questions explicitly. Moreover, there are at least two additional reasons why the present case is not the correct case for entering into that type of discussion.

⁴⁷ For a similar issue in the context of costs for data retention, see the order of 26 November 2020, *Colt Technology Services and Others* (C-318/20, not published, EU:C:2020:969).

95. First, like the number of other issues somehow revolving around the flow of personal data, but not really concerned with the protection of the rights of the data subjects, such issues are simply not specifically regulated by the GDPR. The issue of the legal protection of data controllers – private undertakings against the potentially unlawful or disproportionate interference with their freedom to conduct business, their possible right to property,⁴⁸ or even their potential right to an equitable compensation for the data transferred – is not an issue regulated by the GDPR.

96. Second, so long as the legal basis for such a data transfer is not provided for by EU law,⁴⁹ then the issue of potential compensation for such imposed data transfers can hardly be a matter of EU law either. That is not to say, again, that such issues may not arise, even as a matter of protection of fundamental rights (of the data controllers concerned). However, those issues would then have to be properly addressed by the courts of the Member State imposing such transfers in the first place. Any case of that kind should therefore be brought before a national (constitutional) court.

V. Conclusion

97. I propose that the Court answer the questions referred for a preliminary ruling by the Administratīvā apgabaltiesa (Regional Administrative Court, Latvia) as follows:

- Article 6(1)(c) and (3) 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 does not preclude national rules from laying down, without any limit in time, an obligation for Internet advertising service providers to communicate certain personal data to a tax authority, as long as there is a clear legal basis in national law for such a type of data transfer and the data requested are suitable and necessary for the tax authority to complete its official tasks.

⁴⁸ In increasingly data-driven modern economies, it is only a matter of time before data is recognised as a type of possession, or even property, the same way a number of other immaterial assets of economic value have become, including various types of intellectual property. See, in this regard, the already open stance to the inclusion of various types of ‘possessions’ within the scope of Article 1 of the First Additional Protocol in the case-law of the European Court of Human Rights, as demonstrated, for instance, in judgment of the ECtHR of 11 January 2007, *Anheuser-Busch Inc v. Portugal* (CE:ECHR:2007:0111JUD007304901, §§ 63 to 65).

⁴⁹ As would be, by contrast, the situation in cases where the data transfers, retention or processing are foreseen by an EU law instrument, as is the case with the examples provided above in footnote 36. Incidentally, the original Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC {SEC(2005) 1131}, COM/2005/0438 final – COD 2005/0182, tabled by the Commission, appeared indirectly to acknowledge as much in its originally proposed Article 10 and recital 13. Those provisions, however, were not retained in the adopted version of the directive.