https://doi.org/10.12697/JI.2024.33.04

Monika Mikiver
*Visiting Lecturer of Administrative Law*
*University of Tartu*

Nele Siitam
*Justice, Administrative Law Chamber*
*Supreme Court of Estonia*

# Data-driven Public Administration and the GDPR:

## Seeing the Court of Justice's Judgement in Case C-175/20 in a Broader Context

**Abstract.** Increasingly, public authorities are looking to get the most from their records, with the aid of new technologies that allow them to extract the desired features or patterns from large volumes of data. This could position these authorities well for efficiency and to identify offenders – and, in some cases, future offenders. At the same time, the General Data Protection Regulation lays down the principle of purpose limitation and requires both the European Union and its member states to ensure that the rules by which personal data get processed are foreseeable for the individuals affected. In this context, a distinction must be made between two steps to processing, each with its own issues – the request for or direct access to personal data and mass analysis of the data obtained. The European Court of Justice dealt with several of these after the Latvian tax authority requested 'big data' from a private company. The article examines the guidance that the Court issued in this case (C-175/20) to both national legislators and administrations with regard to the distinct stages of mass processing of data, and it considers which questions remain unanswered.

**Keywords**: data protection, GDPR, purpose limitation, big data and data-mining in public administration, fundamental rights

## 1. Introduction

More and more public authorities are exploring the potential of implementing new technologies that could aid in screening various types of data to identify persons who have failed to comply with their legal obligations or might fail to honour them in the future and to increase the authorities' effectiveness as they carry out their public tasks. Data-screening requires working with several relevant datasets in combination, however, including personal data. This, in turn, raises legal issues and problems as data get requested from other controllers for purposes other than initial processing.

On 24.2.2022, the Court of Justice of the European Union (CJEU) ruled in the case *Valsts ieņēmumu dienests* (C-175/20)[*1] on those provisions of the General Data Protection Regulation[*2] (GDPR) related to

1 Case C-175/20 *SIA 'SS' v Valsts ieņēmumu dienests* EU:C:2022:124.

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) [2016] OJ L119/1.

public administrations' requests for personal data from the private sector. In the case at issue, the Latvian tax authority obliged a provider of Internet-based advertising services to supply the data of its customers who wanted to sell a car via its services. The tax authority required that access to the data be granted either by direct access or through submitting the required data each month. In doing so, Latvia's tax authority relied on Article 15 (6) of the Law on Taxes and Fees, which provides that all providers of online-advertisement services are obliged to provide, at the request of the Latvian tax authority, the information available to them on those taxable persons who have placed advertisements by means of their services.[*3] As to whether this provider of Internet advertising services was afraid of losing the trust of its customers or sources of its own obscured income[*4], one can only speculate. The company might just as well have been afraid of possible responses by the Latvian Data Protection Supervisory Authority, which, for example, had fined an Internet service provider 1.2 million euros in autumn 2022 for passing personal data of its customers onward to a debt-collection company.[*5] In any case, the proprietor lodged a complaint with the tax authority and, after it was rejected, appealed to the Administrative Court to clarify whether the tax authority could legitimately require them to provide such data. The company expressed the view that the tax authority's action violated the GDPR. At this point, the Latvian court referred the case to the CJEU for a preliminary ruling.

A closer look at the ensuing judgement by the CJEU shows that the clarifications given, the references made, and the positions taken by the Court are not specific to tax law. Rather, they have broader relevance for administrative-law relations involving the processing of personal data. This paper, then, written in light of the CJEU's clarifications, examines which requirements are in force for the legal basis for requesting data from another controller or for obtaining direct access to those data, along with the basis for further processing of these data, including examination of efforts to identify useful patterns in large datasets (i.e., data-mining). The modern state needs (personal) data if it wishes to tackle abstract threats to public order as well as to identify those who are already breaching the law or are likely to do so in the future.

## 2. The importance of big data in administrative proceedings

Politicians often want to solve the problems facing society by toughening penalties. However, the reactive, purely punitive approach visible in Estonia's public administration was gradually replaced in the early 2000s by a more preventive approach, with the introduction of an intelligence-led-policing model.[*6] Through intelligence-led policing, the focus of the police shifts from investigating individual crimes to proactive and strategy-oriented forward-looking crime control. This implies an increased emphasis on data's collection and processing, the use of data-analytics technologies[*7], and more widespread use of covert processing of personal data in the early stages of events – before damage occurs.[*8] On account of the emergence of various

3 'Noteikumi par likuma "Par nodokļiem un nodevām" 23. panta otrās un trešās daļas piemērošanu [Regulations on the Application of Section 23 (2) and (3) of the Law On Taxes and Fees]' [1995] (106) Latvijas Vēstnesis <https://www.vestnesis.lv/ta/id/35882-noteikumi-par-likuma-par-nodokliem-un-nodevam-23-panta-otras-un-tresas-dalas-piemerosanu> accessed on 8 July 2024.

4 According to the Latvian press, the implicated provider of Internet-based advertising services has been suspected of playing an important role in the maintenance of the black economy, especially in the context of sales of cars. See A Kulbergs, 'Viedoklis: *ss.lv* spēlē ļoti nopietnu lomu pelēkās ekonomikas uzturēšanā' (*Dienas Bizness*, 7 August 2017) <https://www.db.lv/zinas/viedoklis-sslv-spele-loti-nopietnu-lomu-pelekas-ekonomikas-uzturesana-465294> accessed on 8 July 2024.

5 A summary of the infringement and details of the fine imposed on 9 September 2022 are accessible via GDPRhub: 'DVI (Latvia) – SIA "TET"' <https://gdprhub.eu/index.php?title=DVI_(Latvia)_-_SIA_%22TET%22> accessed on 8 July 2024.

6 For instance, see Priit Suve, 'Kogukonnakeskse politsei roll politsei kujunemisel: arengud Eestis 1991–2013 [The Role of Community Policing in the Development of the Police: Developments in Estonia from 1991 to 2013]' [2014] (5) Acta Politica Estica 42 <http://publications.tlu.ee/index.php/actapoliticaestica/article/view/211> accessed on 8 July 2024.

7 For example, E Aav, who served as Director General of the Tax and Customs Board (in 2006–2011), stressed in 2012: 'The next step in analytical work should be the development of data-collection and forecasting capabilities, which would allow the Board to focus its activities on anticipating and preventing future problems from past events. This will require a serious investment in software.' See 'Enriko Aav: maksuamet peab edasi liikuma [Tax Administration Must Move Forward]' (*Äripäev*, 12 April 2012) <https://www.aripaev.ee/opinion/2012/04/12/enriko-aav-maksuamet-peab-edasi-liikuma> accessed on 8 July 2024.

8 Mait Laaring, 'Eesti korrakaitseõigus ohuennetusõigusena [Estonian Law-Enforcement Law As Threat-Prevention Law]' (PhD thesis, University of Tartu 2015) 19–20 <http://dspace.ut.ee/bitstream/handle/10062/48472/laaring_mait.pdf?sequence=1&isAllowed=y> accessed on 8 July 2024.

new threats, the society of today is often referred to as a 'risk society' and the state's response to it as that of a 'preventive state'.[*9] The increasing focus of other authorities too (alongside the police) on risk prevention is confirmed by, for example, the existence of numerous public-information campaigns centred on how citizens themselves can prevent risks and breaches of the law.

Depending on the sphere of life involved, proactive public administration may require the processing of a large volume of data (that is, working with 'big data') to identify areas wherein the risk of infringement is greater, in aims of designing proactive procedures geared for a more specific target group. Depending on the domain and the situation's particulars, the need might not extend beyond aggregated non-personal data. However, it is often in the administration's interest to process big data, including personal data, in the policy-preparation stage and to 'nip things in the bud': well-executed preparation allows the state to select the 'right' persons for specific procedures while avoiding 'unnecessary' bureaucracy for those who are law-abiding. Via this approach, the rapid development of new technologies makes it possible to utilise different types of data in combination to screen for not only infringers[*10] but also – by means that might even employ artificial intelligence – persons who might end up in breach of legal requirements down the line and who should therefore, at least in the view of state organs, be more closely monitored.[*11]

Although the question of how the Latvian tax authority planned to analyse the requested data[*12] was not addressed in depth in Case C-175/20, it is undisputed that the tax authority had proceeded from a desire to obtain big data from a private company not for the purpose of prosecution for any specific infringement (involving a possible offence) but so as to identify who among the customers obtaining its Internet-based advertising services might be infringers.

# 3. The fundamental-rights framework for the processing of big data

## 3.1. The principle for legality

The fundamental right to privacy (enshrined in § 26 of the Constitution of the Republic of Estonia, or EC) protects individuals from both the collection and the further processing of personal data. Fundamental rights may be restricted only in accordance with the Constitution, with account taken of the principle of legality, which is laid down in Article 3 of the EC and requires that any restriction of a fundamental right must be based on an existing legal foundation.[*13] Article 3 of the EC also lays down the principle of

9 Ibid 20, 23.

10 In the public sector, data-mining is used mostly by financial and tax-supervisory authorities to detect abuses on the basis of 'big data' data structures; see Leonid Guggenberger, 'Einsatz künstlicher Intelligenz in der Verwaltung' [2019] (12) Neue Zeitschrift für Verwaltungsrecht 844, 848. In Estonia, even without the involvement of artificial intelligence, data held by both the tax authorities themselves and the state as a whole are used in detection of tax avoidance in tenancy relationships. See Reet Pärgma and Janno Riispapp, 'Maksuamet nügib üürileandjaid: aastas jääb laekumata kümneid miljoneid [The Tax Office Is Tricking Landlords: Tens of Millions Are Not Collected Every Year]' (*Postimees*, 1 February 2020) <https://majandus24.postimees.ee/6887251/maksuamet-nugib-uurileandjaid-aastas-jaab-laekumata-kumneid-miljoneid?_ga=2.198474540.2039862133.1580404709-1120930609.1394797767>. Among the tax authority's hopes for the future is use of artificial intelligence to create a decision model from mass data for effectively and efficiently ascertaining the likelihood of 'envelope wages' having been paid. See Märt Belkin, 'Maksuamet hakkab tehisintellekti abiga ümbrikupalga maksjaid püüdma [The Tax Authorities Will Use Artificial Intelligence To Catch Payers of Hidden Wages]' (*Rahageenius*, 6 February 2020) <https://raha.geenius.ee/rubriik/uudis/maksuamet-hakkab-tehisintellekti-abiga-umbrikupalga-maksjaid-leidma/>. As for other countries, the French tax authority has offered an example by using artificial intelligence in 2022 to uncover private swimming pools that had gone undeclared, which affect property taxes; see the Euronews piece 'France Uses Artificial Intelligence To Detect More Than 20,000 Undeclared Swimming Pools' (30 August 2022) <https://www.euronews.com/my-europe/2022/08/30/france-uses-artificial-intelligence-to-detect-more-than-20000-undeclared-swimming-pools>. All links accessed on 8 July 2024.

11 For details, see such reports as Kiana Alikhademi and others, 'A Review of Predictive Policing from the Perspective of Fairness' (2022) 30 Artificial Intelligence and Law. – DOI: https://doi.org/10.1007/s10506-021-09286-4.

12 In many countries, data analytics is used to detect tax and benefit fraud. For a more in-depth look at data analysis, as performed by the Latvian tax administration, see Nicolas Gavoille and Anna Zasova, 'Detecting Labor Tax Evasion [by] Using Administrative Data and Machine-Learning Techniques]' (FREE Policy Brief, 17 May 2022) <https://freepolicybriefs.org/wp-content/uploads/2022/05/freepolicybriefs20220517.pdf> accessed on 8 July 2024.

13 See the commentary provided by Madis Ernits on the Constitution of Estonia, s 3, comment 105. <https://pohiseadus.riigioigus.ee/v1/eesti-vabariigi-pohiseadus/i-uldsatted-ss-1-7/ss-3-pohiseaduse-ulimuslikkus-ja-reservatsioon> accessed on 8 July 2024.

importance, under which both the conditions and the scope of any interference must be defined at the level of the law.*[14] Also, in cases of more intensive intervention, the regulation must be more precise than in other cases.*[15]

The Charter of Fundamental Rights (CFR) is an instrument that applies to European Union institutions, bodies, offices, and agencies, but EU member states likewise are bound by the CFR when implementing Union law (under Art. 51 (1) of the charter). The implementation of EU law can take place both in the legislative sphere (through enactment of national law) and in the executive sphere (through the activities of national administrations). As the CFR provides for the right to respect for private life and the right to the protection of personal data (in Art. 7 and Art. 8, respectively)*[16], the CFR is therefore applicable with regard to the GDPR's provisions when a Member State 'complements' the GDPR – i.e., when it creates the legal basis for administrative authorities' processing of personal data. According to the CFR, the exercise of the rights and freedoms recognised under the charter shall be restricted only by actual law and in a manner showing due regard for the nature of those rights and freedoms and the principle of proportionality (per Art. 52 (1)). The right to respect for one's private life and the fundamental right to the protection of personal data are not absolute; they may be restricted by the Member State, subject to Article 52 of the CFR.*[17]

In a recent case pertaining to a directive on public access to information about beneficial ownership, the CJEU explained the content of the principle for a legal basis thus: 'As regards the requirement that any limitation on the exercise of fundamental rights must be provided for by law, this implies that the act which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned', where it must be borne in mind, on one hand, that said requirement 'does not preclude the limitation in question from being formulated in terms [...] sufficiently open to be able to adapt to different scenarios and keep pace with changing circumstances' and, on the other hand, that 'the Court may, where appropriate, specify, by means of interpretation, the actual scope of the limitation in the light of the very wording of the EU legislation in question as well as its general scheme and the objectives it pursues, as interpreted in view of the fundamental rights guaranteed by the Charter'.*[18]

## 3.2. The GDPR: Requirements for a legal basis and purpose limitation

In the CJEU's data-protection jurisprudence, the question of how detailed/general the legal basis for the processing of personal data needs to be to comply with the requirements of the CFR, including what role the nature of the processing operation plays, has not received significant attention thus far.*[19]

According to the GDPR, the processing of personal data is lawful if at least one of the six bases exhaustively listed in Article 6 (1) of the GDPR exists.*[20] In connection with administrative procedure, Article 6 (1)(e) of the GDPR holds relevance. According to it, the processing of personal data is lawful if 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'. Paragraph 3 thereunder specifies that the basis for the processing of personal data referred to here must be established either by Union law or by the law of the Member State

14 Supreme Court Administrative Law Chamber decision 3-3-1-41-00, 31 October 2000, para 4.

15 Supreme Court Administrative Law Chamber decision 3-19-549, 18 May 2021, paras 18, 22.

16 However, the CJEU usually does not distinguish between what articles 7 and 8 of the CFR address. Neither has it clarified whether there are any non-overlapping aspects of the respective fundamental rights. See also Paloma Krõõt Tupay, 'Õigusest eraelule kuni andmekaitse üldmääruseni ehk tundmatu õigus isikuandmete kaitsele [From the Right to Privacy to the GDPR, or the Unknown Right to the Protection of Personal Data]' [2016] (4) Juridica 227.

17 Case C-184/20 *Vyriausioji tarnybinės etikos komisija* EU:C:2022:601, para 70.

18 Joined Cases C-37/20 and 601/20 *Luxembourg Business Registers* EU:C:2022:912, 47; most recently, Case C-61/22 *Landeshauptstadt Wiesbaden*, not reported yet, para 77.

19 The European General Court has recently concluded that a provision of an EU Regulation instrument that generally provides for the possibility of the European Commission requesting the necessary information from undertakings and associations of undertakings constitutes a sufficient legal basis for requesting information (inclusive of personal data) on the Commission's part: Case T-451/20 *Meta Platforms Ireland v Commission* EU:T:2023:276, paras 184–194. However, in *Bara and Others*, the CJEU stated with regard to the legal basis for the transfer of personal data only that it must generally incorporate appropriate safeguards: Case C-201/14 *Bara and Others* EU:C:2015:638, para 28ff.

20 Although it is not excluded that personal data collected by the tax administration may prove necessary also for the purposes of criminal-law proceedings, the activities of the tax administration presumably fall within the scope of administrative law if the facts need to be clarified. Therefore, it is the GDPR, not the Law Enforcement Authorities Directive, that applies, in light of Case C-175/20 (n 1) paras 39–47.

to which the controller is subject, and that either the purpose of the processing must be specified in the relevant legal act or the processing has to 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' with respect to the processing of personal data referred to in paragraph 1 (e) of Article 6. In the case of a special category of personal data, the source of law for the Member State and the additional requirements to be imposed on it should be sought not only in Article 6 but also in Article 9 of the GDPR.[*21] With respect to the legal basis for the processing, Recital 45 of the GDPR does not require each individual processing operation to be governed by a separate legal act, but the legal basis nevertheless must be 'clear and precise[,] and its application should be foreseeable to persons subject to it' (per Recital 41). However, the requirement for a legal basis does not always presuppose a law adopted by the country's parliament – the level of regulation required depends also, *inter alia*, on the constitutional order of the Member State.[*22]

In cases wherein an administrative authority collects personal data from a source other than the individual, by requesting the data either from another administrative authority or from a private person, the purpose-limitation principle too demands consideration, because the purpose behind processing of retained personal data is presumably different from the purpose for which those personal data were initially collected. According to the purpose-limitation principle, which is considered a cornerstone of data-protection law[*23], the processing of personal data must ensure that all personal data's collection is for explicitly specified and legitimate purposes and that the data are not further processed in a way incompatible with those purposes (see Art. 5 (1)(b) of the GDPR).[*24]

The GDPR does, however, allow Member States to regulate the processing of personal data for a different purpose. Authors of various GDPR commentaries have been far from unanimous as to the meaning of the relevant provisions of the GDPR, though. According to Article 6 (2), Member States may maintain pre-existing systems for data-processing in their public administration, while respecting the general framework of the GDPR. It is debatable whether Article 6 (2) constitutes separate delegation to regulate data-processing in the Member State[*25], as opposed to this norm being merely declaratory and, in fact, superfluous[*26], since the real delegation follows from Article 6 (3). The latter allows a Member State to regulate its purpose limitation for the processing of personal data in more detail in connection specifically with the performance of public tasks, with proper specification of 'the entities to, and the purposes for[,] which' the personal data may be disclosed, the purpose limitation involved, etc. There are also some authors who consider the delegation to be derived from sections 2 and 3 of Article 6 in mutual conjunction.[*27]

In addition, Article 6 (4) of the GDPR provides that the processing of personal data for a purpose other than that for which the personal data were collected is permissible under Union or Member State law so long as that processing consists of 'a measure which is necessary and proportionate in a democratic society' to ensure fulfilment of the objectives referred to in Article 23 (1).[*28] Alexander Roβnagel is among the scholars who have found that a distinction must be drawn between situations wherein the legislator regulates purposes that are still compatible with the original purpose and situations in which the legislator regulates processing for a purpose different from the original one. In the first case, the Member State invokes

21 Case C-667/21 *Krankenversicherung Nordrhein* EU:C:2023:433, para 79 (arts 6 and 9 apply cumulatively, not in a relationship between general and specific rules).

22 Per Recital 41 of the GDPR.

23 Article 29 Data Protection Working Party, 'Opinion 03/2013 on Purpose Limitation' (2 April 2013) 4 <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf> accessed on 8 July 2024.

24 Art 8(2) of the CFR also requires that processing of personal data be for 'specified purposes'. In addition, see, for instance, Recital 39 of the GDPR and Recital 26 of the Law Enforcement Agencies Directive, regarding 'specific purpose'; Case C-175/20 (n 1) paras 45, 63–66; Case C73/16 *Puškár* EU:C:2017:725, para 111; Case C-180/21 *Inspector v Inspectorata kam Visshia sadeben savet* EU:C:2022:967; Case C-77/21 *Digi* EU:C:2022:805, para 34; Case C-77/21 EU:C:2022:248, Opinion of AG Pikamäe (31 March 2021), para 37ff. The last of these states that a 'sufficiently precise purpose thus constitutes a fundamental guarantee in terms of predictability and legal certainty in the sense that it contributes to the proper understanding by the data subject of the possible use of his data and enables him to make a fully informed decision'.

25 Alexander Roßnagel in Spiros Simitis, Gerrit Hornung, and Indra Spiecker gen. Döhmann (eds), *Datenschutzrecht: DSGVO mit BDSG* (Nomos 2019) art 6 s 2, marginals 1, 16.

26 Benedikt Buchner and Thomas Petri in Jürgen Kühling and Benedikt Buchner, *Datenschutz-Grundverordnung BDSG Kommentar* (Beck 2020) art 6, marginals 2, 93.

27 Ibid, art 6, marginal 196.

28 For a more in-depth discussion of the problems besetting interpretation of art 6(1–4) of the GDPR, see Monika Mikiver and Paloma Krõõt Tupay, 'Has the GDPR Killed E-government? The "Once-Only" Principle vs the Principle of Purpose Limitation' (2023) 13(3) International Data Privacy Law 194. – DOI: https://doi.org/10.1093/idpl/ipad010.

Article 6 (3) to establish its rules; in the second case, the delegation follows directly from paragraph 4.[*29] The alternative view is that Article 6 (4) does not feature a delegation at all and that delegation follows from the interaction of paragraphs 2, 3, and 4.[*30]

The recitals of the GDPR, which explain, for example, that '[i]f 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' and that '[t]he legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing',[*31] do not shed any particular light on matters to dispel the confusion.

Analysis by the Ministry of Justice of the Republic of Estonia, which dealt with the compatibility of the national regulations on public databases with the EC and with the GDPR, reached the conclusion that a Member State may, on the basis of Article 6 (2)–(3), more precisely regulate the processing of data carried out on the basis of Article 6 (1)'s items (c) and (e) (addressing, respectively, performance of public tasks and legal obligations), concluding also that in this connection the Member State may regulate the purpose limitation too, relying on the provisions of Article 6 (4). In other words, the purpose of the secondary processing must align with the purposes referred to in Article 23 (1) and the regulation must ensure compliance with the principle of proportionality.[*32] In the opinion of the authors of the article, the latter interpretation is fully justified.

## 4. Conclusions about the legal basis and purpose limitation in Case C-175/20

The question as to how general or detailed the legal basis for the access to personal data should be was obviously also a core issue for the referring Latvian court. In fact, the Latvian court seemed to want to know whether Article 15 (6) of the Latvian Law on Taxes and Fees, which provides that 'Internet advertising service providers shall be obliged to provide, upon request of the national tax authority, any information on taxable persons who have used those services for the publication of advertisements and on the advertisements published by them', is 'GDPR-compliant'.

Regrettably, the CJEU did not give a clear answer. From the reasoning of the judgement one can deduce the Court's understanding that it is up to primarily the national legislator to find the right solution in each situation. In other words, it is not excluded that a general legal basis may be permissible in conditions wherein the two levels – the level of the legal basis and the reasoned request – by functioning together constitute an adequate (i.e., GDPR-compliant) legal basis for the processing of personal data.

This position is reflected, firstly, in the Court's reasoning on the question of whether the GDPR's provision for a law that restricts the rights set out in the GDPR points exclusively to a legislative act adopted by Parliament or, instead, is broader in meaning and may cover other legislative acts, adopted by different levels of government, also. On one hand, the Court referred to the CFR, which lays down the principle of legality.[*33] On the other hand, the Court pointed to the above-mentioned recital of the GDPR: Recital 41 is based *expressis verbis* on a broader understanding of what constitutes a legal basis or legislative measure.

Secondly, referring to its previous case law, the CJEU stated that the limitation of rights that is provided for in the GDPR must have a clear and precise legal basis, the limitations' application must be foreseeable

29 Roßnagel (n 27) art 6 s 4, marginal 24.

30 Philipp Reimer in Hjalmar von Sydow, *Europäische Datenschutzgrundverordnung: Handkommentar* (Nomos 2018) art 6, marginal 67; Buchner and Petri (n 28) art 6, marginal 200; Marion Albers and Raoul-Darius Veit in *BeckOK Datenschutzrecht* (Beck 2022) art 6, marginal 77; Horst Heberlein in Eugen Ehmann and Martin Selmayr, *Datenschutz-Grundverordnung DS-GVO Kommentar* (Beck 2018) art 6, marginal 51.

31 Text from Recital 50 of the GDPR.

32 Monika Mikiver, 'Analüüs: Andmekogud ja isikuandmed: EV Põhiseadusest ja IKÜM-st tulenevad nõuded regulatsioonile. Justiitsministeerium 2021 [Analysis: Databases and Personal Data – Regulatory Requirements under the Constitution of the Republic of Estonia and the GDPR]' (Estonian Ministry of Justice 2021) accessible via <https://www.just.ee/uuringud> accessed on 8 July 2024.

33 Case C-175/20 (n 1) para 54.

for the data subjects, and the data subjects must be able to identify the circumstances and conditions under which the scope of the rights conferred on them by the GDPR may be limited.[*34]

After addressing what the general requirements are for a legislative measure that provides for restrictions to the rights set out in the GDPR, the Court's decision turns to other matters, but it later returns to this question when dealing with the sub-topic of the processing of the dataset requested by the Latvian tax administration.[*35] The Court did not say that processing of data in bulk, which might include the granting of direct access for said operation, should be treated more strictly in light of the terms regulating an explicit legal basis. Moreover paragraph 69 of the CJEU judgement makes clear reference to the fact that the authorisation allowing bulk transfer of data must comply with the requirements of Article 6 (1(e) and 3). However, a few paragraphs later (in paragraph 71), the Court seems to concede that it might even be permissible for a detailed rule of authorisation to be entirely absent, so long as a heightened obligation to state reasons with a higher threshold for the administrative body's request stands in its stead.[*36]

Moreover, the CJEU ruling in Case C-175/20 does not address Article 6 (4) of the GDPR, which provides for an exception to the purpose-limitation principle stated in Article 5 (b). Rather than delve into this, the Court found that the legal basis from a Member State's perspective must stem instead from Article 23 of the GDPR, which allows a Member State to limit the rights of the data subject and the obligations of the controller, but also 'Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22'.[*37]

It is regrettable that the judgement does not explain the reasons for the exclusion of Article 6 (4) (in conjunction with Article 6 (2)–(3)) of the GDPR. At the same time, the Court did not specify how to understand the additional conditions for the restriction on Article 5 that are laid down in Article 23 either. There is some question as to whether Article 23 allows a Member State to limit the processing principles set forth in Article 5 as such or, in contrast, the wording of Article 23 makes it instead the rights of the data subject and the obligations of the controller that are subject to said national restrictions. The answer, in turn, affects, for example, the transparency obligation under Article 5.[*38] For instance, a Member State may rely on Article 23 as a basis for restricting the data subject's right to know the precise logic of the profiling of their data, which is what the German legislator has done with regard to such activities as risk assessment in the tax domain[*39]. The legal world is unfortunate also in that the Court did not further elaborate on the content of Article 23 (2) of the GDPR, which lays out in detail the minimum content of such legislation. In rulings prior to the one in Case C-175/20, the CJEU held that any legislative measure adopted under Article 23 (1) GDPR must comply with all the specific requirements comprehensively articulated in Article 23 (2).[*40]

The above reasoning suggests that the CJEU would seem to favour a rather flexible approach to the question of how strict the rules on parliamentary legislation should be. The choice between a special and a general parliamentary law is a matter for the Member State. Such a view is supported also by Recital 41 of the GDPR (which allows space for the constitutional order of the Member State to determine the level of regulation suitable) in conjunction with Recital 45 (the wording of which permits generalisations in the creation of standards). The advantage of a more general legal basis is that the legal regulation necessary for appropriate implementation of the GDPR could be better adapted to the national legal order of the Member States. In particular, it would not lead to 'legal dislocations' – situations wherein, simply because of EU law, a relatively general parliamentary regulation is accepted for extensive or intense interference with fundamental rights while the rules required by law for enabling some forms of less intense invasion must be laid down in detail in a concrete, practice-oriented fashion. One could, of course, offer as a counter-argument that the implementation of the GDPR, as a directly applicable regulation, should not differ very much between Member States.

34 Ibid, paras 55–57.

35 Ibid, paras 83–84.

36 Also Thomas Zerdick, 'EuGH: Datenschutzrecht: Übermittlung von Daten durch Unternehmen an Behörden' [2011] (11) Europäische Zeitschrift für Wirtschaftsrecht 532.

37 Case C-175/20 (n 1) para 51.

38 Also M Bäcker in *Datenschutz-Grundverordnung BDSG Kommentar*, art 23 para 9.

39 For example, under German tax law, the parameters to the algorithm used by the tax-supervisory authority are not published to any degree of precision: 'Details of risk-management systems may not be published where this could jeopardise the uniformity and legality of taxation' (*Abgabenordnung*, s 88(5)).

40 Joined Cases C-511/18, C512/18, and C-520/18 *La Quadrature du Net and others* EU:C:2020:791, para 209.

Irrespective of the choices made by Member States in adopting the measures necessary for the implementation of the GDPR, all of them must meet the criterion presented above as 'foreseeability', which in the Estonian legal tradition entails primarily the adoption of accessible legislative acts.[*41] We hope that the new references for a preliminary ruling will soon give the CJEU an opportunity to 'paint a broader picture', so that it will be easier for Member States to craft and apply GDPR-compliant rules, thereby ensuring stronger protection of fundamental rights.

## 5. Taking the case law on the processing of communications data as a model

As mentioned above, processing of big data varies greatly: it might involve identifying infringers via simple cross-checking between sets of data already held but also can extend to using more sophisticated, AI-based analytics to make predictions and estimations as to who might become an infringer in the future. In any case, working with big data implies 'machine-reading' of data concerning as many people as possible (whether the entire general population or a specific target group). In any context of processing big data, a particularly crucial element is transparency of the personal data's handling[*42], whereby the data subject should be aware of who is processing his or her personal data and for what purpose they are being processed.[*43] This issue has links to the individual's right to verify the accuracy of the data, not least since an error in the source data may get carried forward to other procedures and could affect the assessment of certain characteristics of the data subject. It is precisely because of problems of this kind that, for example, a Dutch court, in a ruling from 5 February 2020, suspended automated risk assessment related to national-tax fraud and labour-law violations.[*44]

Returning our attention to Case C-175/20, we can see that the CJEU based its answer on the questions referred for a preliminary ruling. Those questions dealt with only the request of the tax authorities for big data; therefore, the Court could not tackle the matter of the legal basis for the further processing of the big data collected 'under the belly of' the administrative authority. It is noteworthy that, after the CJEU had listed in its reasoning the requirements for a 'legislative measure' allowing limitation to the rights articulated in the GDPR, the CJEU did, however, refer twice[*45] to its previous judgements addressing processing of communications data (traffic and location data) that is carried out in the context of criminal proceedings or in that of the protection of national security. Namely, the Court explicitly referred to cases C-746/18, *Prokuratuur* (involving criminal proceedings), and C-623/17, *Privacy International* (centred on the right of security and intelligence services to process bulk communications data for the protection of national security).[*46] This manner of attention, of course, raises the question of whether the requirements fleshed out by the CJEU and the ECHR in the areas of surveillance and communications-data processing can (or should) be adhered to in the area of administrative law (and whether they pertain only to the processing of mass data) and, if so, to what extent. If we look at the reasoning provided by the CJEU in Case C-175/20, it is clear that the logic has been modelled on and inspired by cases involving the processing of communications data.

The European Court of Human Rights has a long-standing tradition of case law in the field of surveillance, with which it has developed criteria and requirements for the relevant legal provisions: how precise the substantive presumptions should be; what procedural guarantees must be in place; and under what conditions, for how long, and how the data collected may be used in the future.[*47] The CJEU also

41 See also, for instance, Case C-306/21 *Koalitsia "Demokratichna Bulgaria - Obedinenie"* EU:C:2022:813, paras 46, 50.

42 See art 5(1)(a) ch III s 1, Recital 60.

43 However, this right may be limited by the EU or a Member State under art 23.

44 Jan Horstmann, 'Rechtbank Den Haag: System zur Erkennung von Sozialbetrug verstößt gegen EMRK' [2020] (6) Zeitschrift für Datenschutz-Aktuell, 07047. The judgement of the Dutch court could be found at <https://uitspraken.rechtspraak.nl/#!/details?id=ECLI:NL:RBDHA:2020:865> accessed on 8 July 2024.

45 Case C-175/20 (n 1) paras 55, 83.

46 Case C746/18 *Prokuratuur* EU:C:2021:152, 48; Case C-623/7 *Privacy International* EU:C:2020:790, paras 68, 78.

47 For examples, see *Klass and Others v Germany* App no 5029/71 (ECHR, 6 September 1978); *Association for European Integration and Human Rights and Ekimdzhiev v Bulgaria* App no 62540/00 (ECHR, 28 June 2007); *Kennedy v United Kingdom* App no 26839/05 (ECHR, 18 May 2010); etc.

has amassed extensive case law pertaining to the processing of communications data.*[48] Both surveillance and the processing of communications data are linked to criminal law and procedure. That link extends also to the preliminary stages (proactively combating security threats); however, criminal proceedings and their outcome, whatever it might be (which may be enabled by or decisively influenced by the processing of personal data), generally entail more intense interference with fundamental rights than administrative proceedings/actions do.

The CJEU clarified in Case C-175/20 that collection of personal data that is not limited in time might be permissible by its very nature. The position taken may suggest that there are differences between the processing of communications data and the processing of personal data for administrative purposes, however. One would hope that this is a sign of the emergence of a more nuanced position in administrative law on the question of whether the processing of big data for administrative-law purposes is permissible, when that might be, and what restrictions should be imposed on it.

Processing big data in such a way as to screen specific individuals in or out for the purpose of ascertaining any need for surveillance mechanisms in certain cases implies broad-based invasion of privacy; such retrieval and screening of data on large scale should not be permissible under the general allowances for processing of personal data that are established for specific administrative procedures.*[49] Data-mining of this sort requires a legislative mandate, in which the legislator should set detailed limits to the scope and conditions for the data-processing. The case law developed in the areas of surveillance and communication-data processing can certainly be a source of inspiration here.

# 6. Conclusions

Although Case C-175/20 seems at first glance to be yet another case clarifying the requirements of the GDPR, it gives reason to discuss the boundaries between what is permissible and impermissible in the processing of big data in preparation for administrative proceedings. Indeed, data-mining can, depending on the technology and methodology used, make a significant contribution not only to the fight against serious crime*[50] but also to the prevention of other serious threats to human life and health and to other legitimate interests, allowing better targeting of administrative-law measures. After all, it would be in the public interest to make efficient use of the personal data at the disposal of the state: every paper not needlessly shuffled and every breach of law not committed brings savings for society as a whole. The Estonians have shown innovative progress in the digital services of the state and have set an example for other countries in cutting red tape, through e-services alongside other mechanisms.

However, there is a limit at some point where the interference with people's fundamental rights becomes so great that it outweighs the administrative efficiency sought through such mass data-processing. It is entirely predictable that soon every administrative body will want some kind of 'tool' that, by relying on certain data already available, carries out comparisons among data. One such tool might employ aerial

48 For example, the relevant first judgement of the CJEU: Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* EU:C:2014:238; the latter at the time of writing: C-162/22 *Lietuvos Respublikos generalinė prokuratūra* EU:C:2023:631.

49 For example, the Estonian Administrative Procedure Act provides in s 7(5) that an administrative authority may, for the purpose of administrative acts, measures, or entry into administrative contracts under administrative procedure, process personal data regarding any circumstances necessary for the proceedings in a matter, unless otherwise provided by law or legislation issued pursuant to law. This cannot be considered a sufficient legal basis; see <https://www.riigiteataja.ee/en/eli/505122023003/consolide>. The legal basis for the Estonian Tax Board's collection and screening of personal data held by the state for the purpose of so-called tax intelligence is derived from s 59($1^1$) of the Tax Administration Act, according to which the tax authority of the state has the right to obtain, free of charge and on the basis of a reasoned request, data from the state database that pertain to the real property and other assets owned or held by persons, to the nature and logistics of the economic activities of persons, and to the goods and services related thereto, for the purpose of assessing and analysing the risk of a breach of tax laws or of said act of law and also for the purpose of identifying related persons within the meaning of s 8 of the Income Tax Act. The administrator of the database shall inform the State Tax Administration of any circumstances that render it impossible to comply with the request or that necessitate extending the deadline for complying with the request; see <https://www.riigiteataja.ee/akt/121062024006#para59>. Both links accessed on 8 July 2024.

50 Also, for example, in a decision taken on 16 February 2023, the Federal Constitutional Court of Germany took a position on the Hessian criminal police's data analysis. It found that the authorisation rules allow such IT assistants to serve the legitimate aim of enhancing the fight against serious crime but considered the authorisation rules for the implementation of algorithmic systems to be too general and therefore unconstitutional. See BVerfG, 16.2.2023, 1 BvR 1547/19, 1 BvR 2634/20, para 52ff.

photographs to identify people who have built a fence too close to another building. Another might reveal those who have left their lawn unkempt or have mown it too often. While in the first case the constitutional value at stake is the protection of human life, health, and property (through detection of a breach of fire-safety rules), in the second case any breach might be merely of a code of amenities established for aesthetic reasons. Processing of big data to pave the way for possible administrative proceedings is justified only for the protection of more important legal interests; we must prevent the normalisation of sweeping automated monitoring of individuals.

The CJEU did not take the opportunity that its preliminary ruling in Case C-175/20 offered to clarify in depth the extent of any difference for administrative law between those requirements relevant for the processing of big data for the purpose of preventing an abstract threat and the conditions for the processing of personal data in an individual concrete case. Several of the Court's other conclusions, such as those on the transfer of personal data between controllers, the change of purpose for the processing, and the requirements applicable for a parliamentary law permitting the processing of bulk data, do not provide ultimate clarity either. The restrictions to the scope of privacy that result from increased use of new technologies in the course of performing administrative tasks pose a challenge for the national legislator's seeking of suitable measures: it has to find balance in the intrusion on privacy.[*51]

[51] For example, one option that has been considered in Estonia is to indicate in the administrative decision whether profiling was applied at the time at which it was issued and to identify those databases (of other administrative bodies) whose data were used to inform issuing the administrative decision. See the bill for an act of law amending the Administrative Procedure Act and other, related acts, first proposed on 6 June 2022, 634 SE, s 1 para 3, which fell by the wayside in parliamentary processes <https://www.riigikogu.ee/tegevus/eelnoud/eelnou/21f6df90-a333-413a-a533-ebbf7e9deebe/haldusmenetluse-seaduse-muutmise-ja-sellega-seonduvalt-teiste-seaduste-muutmise-seadus> accessed on 8 July 2024. With regard to the same subject, consult also Mikiver and Tupay (n 28).