Reports of Cases

OPINION OF ADVOCATE GENERAL
SZPUNAR
delivered on 11 May 2023[1]

**Case C-33/22**

**Österreichische Datenschutzbehörde**
**other parties:**
**WK,**
**Präsident des Nationalrates**

(Request for a preliminary ruling from the Verwaltungsgerichtshof (Supreme Administrative Court, Austria))

(Reference for a preliminary ruling – Data protection – Article 16(2) TFEU – Activities falling within the scope of EU law – General Data Protection Regulation – Activities concerning national security – Committee of inquiry of the Parliament of a Member State – Scrutiny of the activity of a police authority – Competence of the data protection supervisory authority – Article 55(1) – Article 77(1) – Direct effect)

## Introduction

1. Do the activities of a committee of inquiry of the Parliament of a Member State fall within the scope of Regulation (EU) 2016/679,[2] particularly when the inquiry concerns matters relating to national security? If so, can the provisions of the GDPR relating to the right to lodge a complaint with a national supervisory authority be applied directly, despite a constitutional principle that precludes external interference in the Parliament's activities? These are, in essence, the questions raised in the present case by the Verwaltungsgerichtshof (Supreme Administrative Court, Austria).

2. In accordance with the case-law of the Court of Justice, I propose to answer in the affirmative. In my view, such a solution would be consistent not only with the intentions of the EU legislature, which established the GDPR as a true *lex generalis* on the protection of personal data, but also with the underlying reasons for the provisions of Article 16 TFEU, the scope of which extends to the supervisory activities of the Member States, such as those at issue in the main proceedings.

[1] Original language: French.

[2] Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ 2016 L 119, p. 1, and corrigendum, OJ 2018 L 127, p. 2) ('GDPR').

3. In the present case, an officer in the criminal police, WK ('the person concerned'), was heard by a committee of inquiry of the Austrian Parliament on the subject of searches carried out, inter alia, at the premises of the Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Federal Office for the Protection of the Constitution and for Counterterrorism, Austria; 'the BVT'). The minutes of the hearing were then published on the Austrian Parliament's website together with the full name of the person concerned, on the grounds that the press had already revealed his identity.

4. Taking the view that his right to confidentiality of personal data had been breached, the person concerned lodged a complaint with the Österreichische Datenschutzbehörde (National Data Protection Authority, Austria; 'the Datenschutzbehörde') under Article 77(1) of the GDPR. However, the substance of the complaint was not examined: the Datenschutzbehörde declared that it did not have the necessary competence, finding that its supervisory power in the present case was incompatible with the constitutional independence of Parliament bodies, given the principle of the separation of powers enshrined in Austrian law.

5. The person concerned therefore commenced proceedings, the outcome of which depends on the answers to the questions referred to the Court of Justice for a preliminary ruling. Those questions relate, in essence, to the material scope and the direct effect of the relevant provisions of the GDPR, the content of which is set out below.

## Legal framework

### *European Union law*

6. Recitals 16, 20 and 117 of the GDPR state:

'(16) This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

…

(20) While this Regulation applies, inter alia, to the activities of courts and other judicial authorities, Union or Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities. The competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. …

…

(117) The establishment of supervisory authorities in Member States, empowered to perform their tasks and exercise their powers with complete independence, is an essential component of the protection of natural persons with regard to the processing of their personal data. Member States should be able to establish more than one supervisory authority, to reflect their constitutional, organisational and administrative structure.'

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

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

2. This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

…'

8. Article 23(1) of the GDPR, entitled 'Restrictions', provides:

'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:

(a) national security;

…

(h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

…'

9. Article 51(1) of the GDPR, entitled 'Supervisory authority', reads as follows:

'Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the

fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union ("supervisory authority").'

10. Article 55 of the GDPR, entitled 'Competence', reads as follows:

'1. Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

…

3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.'

11. Article 77(1) of the GDPR, headed 'Right to lodge a complaint with a supervisory authority', states:

'Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, … if the data subject considers that the processing of personal data relating to him or her infringes this Regulation.'

### *Austrian law*

12. Article 53 of the Bundes-Verfassungsgesetz (Federal Constitutional Law) of 2 January 1930 (BGBl. 1/1930), in the version of 30 December 2021 (BGBl. I 235/2021), provides:

'(1) The National Council can by resolution set up committees of inquiry. In addition, a committee of inquiry must be set up on demand of one quarter of its members.

(2) The subject matter of the investigation is a certain completed process regarding matters in which the Federation is responsible for implementing the laws. This includes all activities of executive bodies or officers of the Federation through which the Federation exercises rights associated with holding an economic interest and supervisory rights irrespective of the proportion of its interest. An examination of jurisdiction is excluded.

(3) All executive bodies or officers of the Federation, the provinces, the municipalities and the municipal associations and of the other self-administering bodies shall submit to a committee of inquiry, on demand, their files and documents to the extent to which these relate to the subject matter of the investigation and shall comply with the request of a committee of inquiry to take evidence in connection with the subject matter of the investigation. …

…'

13. As provided in Paragraph 18(1) of the Datenschutzgesetz (Law on the protection of personal data) of 17 August 1999 (BGBl. I 165/1999), in the version of 26 July 2021 (BGBl. I 148/2021; 'DSG'), entitled 'Establishment':

'The Datenschutzbehörde is established as a national supervisory authority pursuant to Article 51 of the GDPR.'

14. Paragraph 24 of the DSG, entitled 'Complaints with the Datenschutzbehörde', reads as follows:

'(1) Every data subject has the right to lodge a complaint with the Datenschutzbehörde if the data subject is of the opinion that the processing of the personal data concerning the data subject infringes the GDPR …'

15. Paragraph 35 of the DSG, entitled 'Specific powers of the Datenschutzbehörde', provides, in subparagraph 1:

'The Datenschutzbehörde shall safeguard data protection in accordance with the detailed provisions of the GDPR and this federal law.'

## The facts giving rise to the dispute, the main proceedings and the questions referred for a preliminary ruling

### *Background to the dispute*

16. On 20 April 2018, the lower house of the Austrian Parliament set up a committee of inquiry to examine the alleged influence exerted on the BVT with a view to exploiting its activities. The allegations, which were made by the members of parliament who called for an investigation, concerned, in particular, instances of alleged abuse of authority by BVT staff, rumours of wiretapping in the offices of the Federal Chancellery, the alleged exploitation of investigations targeting certain extremist movements, and politically motivated appointments within the BVT and in ministerial offices.

17. On 19 September 2018, the person concerned was heard by the committee of inquiry as a witness. As an officer of a federal police task force responsible for fighting street crime, he was questioned about searches and seizures of data that his unit carried out at the BVT's offices and in the homes of its employees.

18. Despite the practice adopted in respect of several other witnesses, and notwithstanding the request for anonymity submitted by the person concerned, the committee of inquiry revealed his identity by publishing the full version of the minutes of the hearing on the Austrian Parliament's website.

### *Proceedings in the main action*

19. The complaint lodged by the person concerned with the Datenschutzbehörde under Article 77(1) of the GDPR was rejected on the ground of lack of competence. In its decision of 18 September 2019, that authority stated that the principle of the separation of powers precluded it from interfering in the activities of a Parliament body.

20. The action brought by the person concerned against the decision of 18 September 2019 was upheld by the Bundesverwaltungsgericht (Federal Administrative Court, Austria) by judgment of 23 November 2020. That court annulled the decision of the Datenschutzbehörde on the ground that the GDPR did not provide for exceptions that might limit its scope with regard to legislative bodies.

21. The Datenschutzbehörde brought an appeal on a point of law against that judgment before the Verwaltungsgerichtshof (Supreme Administrative Court), which queries whether the provisions of the GDPR can apply in the main proceedings.

### *Questions referred for a preliminary ruling*

22. First – and irrespective of the subject matter of the inquiry in the main proceedings – the referring court questions whether the activities of a parliamentary committee of inquiry 'fall within the scope of Union law' within the meaning of Article 16(2) TFEU. This provision determines the competence of the European Parliament and the Council to adopt rules on the processing of personal data by the Member States.

23. In that respect, in so far as the competences of the European Union remain limited by the principle of conferral, the referring court wonders whether the GDPR is intended to apply to the activities of a parliamentary body entrusted with the task of political scrutiny, which do not seem to be governed by any specific provision of EU law.

24. Mindful of the need to preserve the national identity and essential functions of the Member States, in accordance with Article 4(2) TEU, the referring court also observes that interference by an administrative body, such as the Datenschutzbehörde, in the activities of the Parliament would contravene the principle of the separation of powers enshrined in the Austrian Constitution.

25. Furthermore, in the light of the judgment in *Land Hessen*,[3] in which the Court of Justice confirmed that the provisions of the GDPR applied to the activities of the Petitions Committee of the Parliament of Land Hessen, the referring court wonders whether the tasks of the Petitions Committee, which contributes only indirectly to parliamentary activities, should not be distinguished from those of committees of inquiry which, according to the referring court, are central to the activities of the Parliament and could therefore fall outside the scope of EU law.

26. Second, if the Court of Justice were to find that the provisions of the GDPR are intended to govern the activities of committees of inquiry, the referring court asks whether the committee at issue in the main proceedings should not be excluded, in so far as its activities are related to matters of national security.

27. On that point, the referring court observes that, according to recital 16 of the GDPR, 'activities concerning national security' do not fall within the scope of that regulation. In its view, that might be the case with the investigation into the political pressure exerted on the BVT, the federal body responsible for safeguarding the essential functions of the State.

28. Third, if the Court of Justice were to conclude that the provisions of the GDPR do apply in the present case, the referring court queries the direct application of that regulation.

29. In the absence of an appropriate constitutional exemption, the competence of the Datenschutzbehörde remains limited by the principle of the separation of powers which prevails in Austrian law. Accordingly, the referring court wonders whether the competence of that authority with regard to the bodies of the Austrian Parliament could arise directly from the

[3] Judgment of 9 July 2020 (C-272/19, EU:C:2020:535).

combined provisions of Article 77(1) and Article 55(1) of the GDPR, when the national legislature has established only a single supervisory authority under Article 51(1) of that regulation.

30. In that context, the Verwaltungsgerichtshof (Supreme Administrative Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

'(1) Do activities of a committee of inquiry set up by a Parliament of a Member State in the exercise of its right to scrutinise the executive fall within the scope of EU law within the meaning of the first sentence of Article 16(2) TFEU, irrespective of the subject matter of the inquiry, with the result that [the GDPR] is applicable to the processing of personal data by a parliamentary committee of inquiry of a Member State?

If Question 1 is answered in the affirmative:

(2) Do activities of a committee of inquiry which has been set up by a Parliament of a Member State in the exercise of its right to scrutinise the executive and which has as the subject matter of its inquiry the activities of a police State-protection authority, that is to say, activities concerning the protection of national security within the meaning of recital 16 of the GDPR, come within the scope of the exception set out in Article 2(2)(a) of the GDPR?

If Question 2 is answered in the negative:

(3) If – as in the present case – a Member State has established only one single supervisory authority in accordance with Article 51(1) of the GDPR, does the competence of that authority in respect of complaints within the meaning of Article 77(1) of the GDPR, in conjunction with Article 55(1) thereof, already arise directly from the GDPR?'

31. Written observations were submitted by the person concerned, the Präsident des Nationalrates (President of the National Council, Austria), the Datenschutzbehörde, the Austrian and Czech Governments and the European Commission. The same parties were represented at the hearing held on 6 March 2023.

## Assessment

### *The first question referred*

32. By its first question, the referring court asks whether the activities of a committee of inquiry set up by a Parliament of a Member State in the exercise of its right to scrutinise the executive fall within the scope of EU law within the meaning of the first sentence of Article 16(2) TFEU.

33. The answer to that question first depends on the interpretation to be given to the concept of 'activities which fall within the scope of Union law', as referred to in the first sentence of Article 16(2) TFEU. Expressed in negative terms, the same concept is also found in Article 2(2)(a) of the GDPR, which excludes from the application of that regulation '[activities] which [fall] outside the scope of Union law'. Those two provisions delineate, respectively, the competence of EU bodies to adopt rules relating to the protection of personal data and the material scope of the GDPR.

34. The answer to the first question also depends on how the activities of parliamentary committees of inquiry should be characterised in the light of the abovementioned provisions of the TFEU and GDPR.

*The concept of 'activities falling within the scope of Union law'*

35. As I endeavoured to show in another case,[4] that concept is not unequivocal, in so far as it lends itself to two different interpretations. In view of the debate surrounding its interpretation in the present case, despite the settled case-law of the Court of Justice,[5] it seems to me to be necessary to set out in detail the reasons for the developments in case-law in this area.

– *Concretising interpretation*

36. The first of the possible interpretations of the 'scope of Union law' can be described as concretising, in the sense that it raises the question of whether a given activity is covered by a specific provision of EU law.

37. In essence, that interpretation corresponds to the concept of 'implementation of Union law', which defines the scope of application of the Charter of Fundamental Rights of the European Union ('the Charter'). In a context unrelated to data protection, that concept is equated with the 'scope of Union law' in the case-law of the Court of Justice.[6]

38. The referring court relies on that interpretation in its request for a preliminary ruling. It notes that the activities of parliamentary committees of inquiry remain governed exclusively by national law, causing it to doubt whether the GDPR is intended to be applied in the main proceedings.

39. Advocate General Tizzano also relied on the same interpretation in his Opinion in joined cases *Österreichischer Rundfunk and Others*[7] and in *Lindqvist*,[8] within the scope of application of Directive 95/46/EC.[9] Those Opinions were not followed by the Court of Justice.

40. It should be noted that Directive 95/46 was adopted on the basis of the former Article 100a of the EC Treaty, which became Article 95 EC, and later Article 114 TFEU, in the context of measures which had as their object the establishment and functioning of the internal market. Seeking to ensure the free movement and equivalent level of protection of personal data within the European Union, that directive was not applicable, under Article 3(2) thereof, to activities which '[fell] outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public

4 See my Opinion in *Latvijas Republikas Saeima (Penalty points)* (C-439/19, EU:C:2020:1054, point 44 et seq.).

5 See judgments of 20 May 2003, *Österreichischer Rundfunk and Others* (C-465/00, C-138/01 and C-139/01, EU:C:2003:294); of 6 November 2003, *Lindqvist* (C-101/01, EU:C:2003:596); of 9 July 2020, *Land Hessen* (C-272/19, EU:C:2020:535); and of 22 June 2021, *Latvijas Republikas Saeima (Penalty points)* (C-439/19, EU:C:2021:504).

6 Judgments of 26 February 2013, *Åkerberg Fransson* (C-617/10, EU:C:2013:105, paragraph 21); of 21 December 2016, *AGET Iraklis* (C-201/15 EU:C:2016:972, paragraph 62); of 21 May 2019, *Commission* v *Hungary (Usufruct over agricultural land)* (C-235/17, EU:C:2019:432, paragraph 63); and of 24 September 2020, *YS (Occupational pensions of managerial staff)* (C-223/19, EU:C:2020:753, paragraph 78).

7 C-465/00, C-138/01 and C-139/01, EU:C:2002:662.

8 C-101/01, EU:C:2002:513.

9 Directive of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31.). This directive was replaced by the GDPR.

security, defence, State security … and the activities of the State in areas of criminal law', or to data processing carried out 'by a natural person in the course of a purely personal or household activity'.

41. In the light of those provisions, Advocate General Tizzano concluded that Directive 95/46 could not apply in *Österreichischer Rundfunk and Others*.[10] With regard to the processing of data on salaries paid by public entities, to be included in a report sent to the Parliament by the Austrian Court of Auditors, he thus determined that, in that instance, the Austrian Court of Auditors was undertaking a 'public-audit activity prescribed and regulated by the Austrian authorities (and in fact in a constitutional law) on the basis of a choice of a policy and institutional nature made by them autonomously and not intended to give effect to a Community obligation. Since it is not the subject of *any specific Community legislation*, that activity can only fall within the competence of the Member States'.[11]

42. Following the same interpretation in *Lindqvist*, Advocate General Tizzano considered that the webpage set up by Mrs Lindqvist as part of her voluntary work as a catechist fell within the scope of 'a non-economic activity which had no connection (or at least no direct connection) with the exercise of the fundamental freedoms protected by the Treaty and is not governed by any specific rules at Community level'.[12] According to the Advocate General, that activity was therefore outside the scope of Community law within the meaning of Article 3(2) of Directive 95/46.

43. That Opinion was not followed by the Court of Justice, for reasons linked to the preservation of legal certainty and the need to ensure the effectiveness of Directive 95/46.

44. Given the specific nature of personal data, the movement and economic exploitation of which are facilitated by their digitisation, it is very difficult to ascertain in practice, on a case-by-case basis, whether their processing is linked to particular provisions of EU law or to the freedoms governing the internal market, as a concretising interpretation would require.

45. To return to the example of the case giving rise to the judgment in *Lindqvist*,[13] it would be difficult to ascertain in practice whether the operation of a webpage intended for a small group of parishioners was specifically linked to the provisions of Directive 95/46 on the free movement of data between Member States within the common market. The answer to this question may depend, inter alia, on the physical location of the servers hosting the website in question.[14]

46. I would add that similar difficulties might arise if the concretising interpretation were to prevail in the present case under the GDPR.

10 C-465/00, C-138/01 and C-139/01, EU:C:2002:662.

11 Opinion of Advocate General Tizzano in joined cases *Österreichischer Rundfunk and Others* (C-465/00, C-138/01 and C-139/01, EU:C:2002:662, point 43). Emphasis added.

12 Opinion of Advocate General Tizzano in *Lindqvist* (C-101/01, EU:C:2002:513, point 36).

13 Judgment of 6 November 2003 (C-101/01, EU:C:2003:596).

14 On this question, see judgment of 6 November 2003, *Lindqvist* (C-101/01, EU:C:2003:596, paragraph 59).

47. By way of illustration, it would be hard to pinpoint to what extent the activities of certain controllers – such as churches or religious associations, which are explicitly covered by that regulation [15] – do in fact remain subject to specific provisions of EU law. [16] The same question might arise for non-profit organisations that do not engage in economic activities. This would result in legal uncertainty as to the scope of the GDPR.

48. In view of those difficulties, the Court of Justice rejected the concretising interpretation of the 'scope of Community law' under Directive 95/46. In the judgments in *Österreichischer Rundfunk and Others* [17] and *Lindqvist*, [18] it held that 'since any personal data can move between Member States, Directive 95/46 requires in principle compliance with the rules for protection of such data with respect to any processing of data as defined by Article 3. … In those circumstances, the applicability of Directive 95/46 cannot depend on whether the specific situations at issue … have a sufficient link with the exercise of the fundamental freedoms guaranteed by the Treaty … A contrary interpretation could make the limits of the field of application of the directive particularly unsure and uncertain, which would be contrary to its essential objective of approximating the laws, regulations and administrative provisions of the Member States in order to eliminate obstacles to the functioning of the internal market deriving precisely from disparities between national legislations'. [19]

49. Thus, the 'generalising' interpretation of Directive 95/46 has prevailed in the case-law of the Court of Justice.

– *Generalising interpretation*

50. The generalising interpretation entails the inclusion in the scope of EU law of all activities that *are capable of* falling within it, in the sense that they have not been excluded from it on account of the Member States' exclusive competence.

51. Under Directive 95/46, that interpretation led the Court of Justice to a narrow reading of the exception relating to activities which were outside the scope of Community law. In the judgment in *Lindqvist*, the Court thus held that 'the activities mentioned by way of example in the first indent of Article 3(2) of Directive 95/46 are intended to define the scope of the exception provided for there, with the result that that exception applies only to the activities which are expressly listed there or which can be classified in the same category (*ejusdem generis*)'. [20]

52. Prior to the entry into force of the Treaty of Lisbon, the activities covered by that exception – concerning public security, defence, State security and crime, as well as those referred to in Titles V and VI of the Treaty on European Union – came under the second and third pillars of the Union and were thus covered by intergovernmental cooperation. Therefore, those activities could not be governed by EU legislation, given the allocation of competences between the European Union and the Member States provided for at the time by the Treaties.

15 See Article 91 of the GDPR.

16 On the one hand, EU law is not intended to specifically govern religious activities. On the other hand, such activities still have to comply with EU law and its general principles, such as the principle of non-discrimination. On that question, see Opinion of Advocate General Tanchev in *Egenberger* (C-414/16, EU:C:2017:851, points 46 to 51).

17 Judgment of 20 May 2003 (C-465/00, C-138/01 and C-139/01, EU:C:2003:294).

18 Judgment of 6 November 2003 (C-101/01, EU:C:2003:596).

19 Judgment of 20 May 2003, *Österreichischer Rundfunk and Others* (C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraphs 40 and 42). See also judgment of 6 November 2003, *Lindqvist* (C-101/01, EU:C:2003:596, paragraph 40 et seq.).

20 Judgment of 6 November 2003, *Lindqvist* (C-101/01, EU:C:2003:596, paragraph 44).

53. It is in that context that the exclusion of 'an activity which falls outside the scope of Community law' contained in the first indent of Article 3(2) of Directive 95/46 must be read. As it is, the scope of the GDPR has been defined in similar terms.

54. According to Article 2(2)(a) to (d) of the GDPR, that regulation does not apply to the processing of personal data '(a) in the course of an activity which falls outside the scope of Union law; (b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU; (c) by a natural person in the course of a purely personal or household activity; (d) by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security'. The latter type of processing is subject to the provisions of Directive (EU) 2016/680. [21]

55. In the light of recital 16 of the GDPR, activities which fall outside the scope of EU law are, inter alia, those concerning national security.

56. On the basis of all of those provisions, the Court of Justice held in *Land Hessen* that the exception provided for in Article 2(2)(a) of the GDPR, covering 'activities which fall outside the scope of Union law', is to be interpreted strictly, so that the 'fact that an activity is an activity characteristic of the State or of a public authority is not sufficient ground for that exception to be automatically applicable to such an activity. It is necessary that that activity is one of the activities that are *explicitly mentioned* by that provision or that it can be *classified in the same category* as those activities'. [22]

57. None of the arguments raised in the present case seem likely to call that interpretation into question.

58. Specifically, I do not agree with the arguments based on the principle of conferral, which were raised, in particular, by the referring court and by the President of the National Council.

59. In accordance with the principle of conferral set out in Article 5(2) TEU, [23] the European Union has only competences conferred upon it in the Treaties by the Member States.

60. From a purely lexical point of view, the concept of 'activities which fall within the scope of Union law' is ambiguous in that respect. At first glance, the generalising interpretation of this concept adopted in the case-law of the Court of Justice might seem questionable, in so far as it results in all activities that have not been excluded from the GDPR being made subject to the provisions of that regulation, which seems contrary to the abovementioned principle.

[21] Directive 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).

[22] Judgment of 9 July 2020, *Land Hessen* (C-272/19, EU:C:2020:535, paragraph 70). Emphasis added.

[23] As a reminder, Article 5(2) TEU provides that: 'under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States.'

61. However, according to settled case-law, the interpretation of a provision of EU law requires that account be taken not only of its wording and the objectives it pursues, but also of its context and the provisions of EU law as a whole. The origins of a provision of EU law may also provide information relevant to its interpretation. [24]

62. Yet leaving aside the literal interpretation, which seems inconclusive in the light of the ambiguous wording of the 'scope of Union law', the contextual [25] and teleological analysis clearly militates in favour of the generalising interpretation of Article 16(2) TFEU, such that the scope of that provision goes beyond that of 'implementing Union law' within the meaning of Article 51(1) of the Charter.

63. First, this conclusion is inevitable in view of the systematic nature of the TFEU and the special place of Article 16(2) in the architecture of that Treaty.

64. The article in question is found in Title II of Part One of the TFEU, containing 'provisions having general application'. It follows that the right of natural persons to the protection of personal data, enshrined in that provision, is of singular importance compared with the other fundamental rights included in the Charter annexed to the Treaty.

65. More specifically, the privileged position of Article 16 TFEU in the scheme of the Treaty suggests that the 'scope' referred to in that provision is not limited to situations where Member States 'are implementing Union law' within the meaning of Article 51(1) of the Charter, which would correspond to the concretising interpretation described above.

66. On that point, I would stress that there is an inherent difference between the provisions of Article 16(2) TFEU and the provisions of the Charter.

67. Under Article 51(2) of the Charter, the Charter does not 'establish any new power or task for the Union, or modify powers and tasks as defined in the Treaties'. Its provisions are addressed to the Member States, in so far as they are implementing EU law in areas which already fall within the scope of that law.

68. It is a different matter for Article 16(2) TFEU, the provisions of which *constitute and delegate* to the Union legislative competence for the protection and free movement of personal data, and to that end define a specific scope, based on the provisions of Directive 95/46, as attested by the origins of that provision.

69. Second, it is clear from the preparatory work for the Treaty of Lisbon that the authors of the TFEU intended to reaffirm the scope of the rules on the protection of personal data, as defined under Directive 95/46.

70. It is worth noting that the wording of Article 16 TFEU is directly inspired by the draft Treaty establishing a Constitution for Europe, Article 36a(2) of which (which became Article 50(2) in the final version of the draft of 18 July 2003) [26] provided for the competence of Parliament and the

[24] For an illustration, see judgment of 10 December 2018, *Wightman and Others* (C-621/18, EU:C:2018:999, paragraph 47 and the case-law cited).

[25] By this I mean an interpretation based on systematic and historical considerations, in accordance with the generally accepted types of interpretation methods (see Lenaerts, K., and Gutierrez-Fons, J. A., *Les méthodes d'interprétation de la Cour de justice de l'Union européenne*, Bruylant, Brussels, 2020, Chapter I).

[26] Draft Treaty establishing a Constitution for Europe (OJ 2003 C 169, p. 1).

Council to adopt 'the rules relating to the protection of individuals with regard to the processing of personal data by the Union's institutions and bodies, and *by the Member States when carrying out activities which come under the scope of Union law*, and the rules relating to the free movement of such data'. [27]

71. However, according to the explanations given by its authors, 'draft Article 36a is intended to create a single legal basis for personal data protection, for the protection of such data by both the institutions and the Member States when they are acting in areas covered by the scope of Union law. *The text is based on the current Community system, stemming from [Directive 95/46/EC]* (based on Article 95 TEC) *as regards the actions of the Member States*'. [28]

72. Clearly, it follows that if the concept of 'scope of Union law' in Article 2(2)(a) of the GDPR were to be interpreted in such a way as to restrict the application of that regulation compared with Directive 95/46, this would be contrary to the intention of the Member States as expressed in the TFEU.

73. Third, consideration should be given to the teleological aspects, linked to the dynamics and specific objectives of personal data protection which underpin the adoption of the GDPR.

74. From that perspective, there is no doubt that the EU legislature has sought to strengthen that protection and to consolidate the scope of the relevant rules. This is evident from the deliberate replacement of Directive 95/46 by a more binding regulatory system and, explicitly, the content of recitals 9, 11 and 13 of the GDPR.

75. The objectives referred to in that measure stem from the specific nature of the phenomenon of data processing, which goes beyond the scope of the activities in which such data may be collected.

76. Moreover, such activities are not necessarily economic activities, which would already be subject to the rules of EU law that govern the internal market. This in no way diminishes the market value of the data collected and does not remove the risks associated with processing those data.

77. The issues relating to personal data are cross-cutting in that respect, such that the rules on data protection cannot be confined to the scope of pre-existing categories of EU law.

78. In other words, if the 'scope of Union law' referred to in Article 16(2) TFEU goes beyond the cases of 'implementing Union law' within the meaning of Article 51(1) of the Charter, it is because the issues linked to the processing of personal data are self-contained and call for a specific legislative measure whose scope exceeds the sum of the pre-existing provisions of EU law. From this point of view, the broad scope of the GDPR reflects the intention to address the challenges of personal data protection by the adoption of a 'customised' scheme.

[27] Article 36a(2) of Draft Title VI of the Constitutional Treaty concerning the democratic life of the Union (Note from the Praesidium of the European Convention to the Convention of 2 April 2003, Brussels, CONV 650/03, p. 6). Emphasis added.

[28] Note from the Praesidium of the European Convention to the Convention of 2 April 2003, Brussels, CONV 650/03, p. 3. Emphasis added.

79. Given the convergence in the findings that emerge from the contextual and teleological analysis of Article 16(2) TFEU, I propose that the Court of Justice confirm its previous case-law [29] by adopting a strict interpretation of the exception relating to an 'activity which falls outside the scope of Union law', contained in Article 2(2)(a) of the GDPR.

80. I propose that the Court of Justice assess the applicability of that regulation to the activities of the parliamentary committee of inquiry at issue in the main proceedings in the light of that interpretation.

*The application of the GDPR to the activities of the parliamentary committee of inquiry*

81. I shall begin with a preliminary observation on how the relevant provisions of the GDPR define the scope of that regulation.

– *The secondary importance of institutional criteria for defining the scope of the GDPR*

82. It should be stressed that organic or institutional considerations as to the nature of the bodies or persons responsible for processing personal data are of secondary importance in defining the scope of the GDPR.

83. First, the scope of the GDPR is based on the material concept of 'processing' of personal data under Article 2(1) of that regulation. From that perspective, the organic concept of 'controller' contained in Article 4(7) of the GDPR is merely ancillary, in the sense that it is based, in essence, on the material concept of processing. Although the definition of controller refers to 'the natural or legal person, public authority, agency or other body', that description has the effect of neutralising the organic criteria for the purposes of its application.

84. Second, even though the provisions limiting the material scope of the GDPR, contained in Article 2(2) of that regulation, refer to certain categories of persons or bodies – namely Member States, natural persons and authorities competent in criminal matters – it is always in the context of *activities* which are not covered by that regulation. Therefore, it is not individuals as such who are exempt from the application of the GDPR, but only some of their activities.

85. The secondary importance of institutional criteria is also confirmed by the way in which partial exemptions, which limit the scope of the specific provisions of the GDPR, are defined. By way of illustration, [30] while courts fall outside the competence of the national supervisory authorities, under Article 55(3) of the GDPR, they do so only to the extent that they *are acting in their judicial capacity*. The scope of this exception is thus determined not by the status of judicial bodies, but by the particular nature of their activities.

86. In the absence of any provision of the GDPR that specifically refers to parliamentary bodies, it follows, in my view, that it is not the *status of parliamentary bodies* in Austrian law but the *nature of their activities* that must determine the possibility of applying that regulation.

[29] See case-law cited in footnote 5 above.

[30] See also Article 20(3), Article 49(3) and Article 79(2) of the GDPR.

– *The nature of the activities of the committee of inquiry in the main proceedings*

87. In the light of all the information before the Court of Justice, I consider that the tasks entrusted to that committee may be classified as activities of public oversight involving the exercise of official authority.

88. That classification is apparent from the very content of the first and second questions referred for a preliminary ruling, which concern activities carried out in the context of *scrutinising* the executive. According to the explanations provided by the referring court, 'the aim of committees of inquiry is to shed light on certain points for political purposes. In that respect, committees of inquiry have a duty to fulfil the *supervisory role* conferred on them by the Constitution'. [31]

89. This characterisation is corroborated by the written observations submitted to the Court. [32]

90. In the light of the explanations given at the hearing by the President of the National Council, it is also common ground that the committee of inquiry in question has certain prerogatives as a public authority, such as the right to summon witnesses or access documents relating to the subject matter of its activities, together with the power to impose financial penalties in order to ensure the proper conduct of the inquiry.

91. Conversely, there seems to be some confusion regarding the *legislative* nature of the committee's activities and its possible consequences for the applicability of the GDPR.

92. The President of the National Council observes in that respect that from an organisational and a functional point of view, 'committees of inquiry are part of the legislature. Actions taken by or on behalf of committees of inquiry thus fall within the legislative function of the State'. [33] In the National Council's view, it follows that 'the work of a committee of inquiry is central to the legislative process and, as a (supervisory) activity which is exclusively parliamentary and political in nature, it falls within the exception provided for in Article 2(2)(a) of the GDPR'. [34]

93. I have three observations to make with regard to those statements.

94. First, regardless of whether committees of inquiry are involved in the legislative process, I should point out that legislative and parliamentary activities have not been excluded from the application of the GDPR, [35] unlike activities linked to the exercise of judicial functions, which fall under the partial exemption provided for in Article 55(3) of that regulation.

95. On this point, unlike some interested parties, I doubt that that exemption can be interpreted by analogy, extending the exception that applies to judicial functions to legislative functions. On the contrary, if the exemption contained in Article 55(3) of the GDPR were to guide the Court of Justice in its reasoning in the present case, it could only lead to an interpretation *a contrario*. Given the wide scope of the GDPR, the exception for judicial functions cannot be broadly construed.

[31] Paragraph 25 of the request for a preliminary ruling. Emphasis added.

[32] By way of illustration, in paragraph 13 of his written observations, the President of the National Council explains that the Austrian Parliament 'may decide to set up committees of inquiry for the purpose of investigating certain acts within the remit of the executive at the federal level. The Constitution thus confers a supervisory role on a committee of inquiry. The aim of a committee of inquiry is to clarify, for political purposes, the course of certain events and thus ensure effective parliamentary scrutiny'.

[33] Paragraph 14 of the written observations of the President of the National Council.

[34] Paragraph 15 of the written observations of the President of the National Council.

[35] See judgment of 9 July 2020, *Land Hessen* (C-272/19, EU:C:2020:535, paragraph 72).

96. Second, in my view, none of the evidence before the Court of Justice supports the argument that the activity of the committee of inquiry in the main proceedings has a legislative function.

97. In particular, the committee of inquiry in question is not empowered to take legislative initiatives and does not otherwise participate in the legislative activities of the Austrian Parliament. Moreover, even though the final report of the committee of inquiry may guide the legislature, that circumstance does not seem to me to make its activities legislative in nature. The activities of some extra-parliamentary bodies – such as the Austrian Court of Auditors, whose reports are sent to the Parliament – might also guide the legislature, without them thereby being associated with the exercise of legislative power.

98. Third, and irrespective of their possible significance under Austrian law, institutional considerations do not affect the applicability of the GDPR. Therefore, the organisational framework of the parliamentary committee of inquiry does not determine the answer to be given to the first question referred for a preliminary ruling.

– *The applicability of the GDPR to public oversight activities*

99. In the light of the above considerations, the question arises whether public oversight activities carried out by a parliamentary committee of inquiry fall within the scope of the GDPR.

100. I believe that this question should be answered in the affirmative, for three main reasons.

101. First, the processing of personal data by the committee in question falls within the material concept of 'processing', as defined in Article 2(1) of the GDPR. That characterisation is not contested by any of the parties in the present case.

102. Second, public oversight activities fall within the scope of EU law within the meaning of Article 16(2) TFEU and Article 2(2)(a) of the GDPR, as interpreted in the case-law of the Court of Justice, in so far as they are not excluded from its application by any provision of that regulation.

103. On the contrary, explicit reference is made to oversight activities in Article 23(1)(h) of the GDPR, which allows for the possibility of *restricting* the scope of certain rights and obligations provided for in that regulation, where such a restriction is necessary to safeguard 'a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority' in certain cases envisaged in that article.

104. It follows that the provisions of the GDPR are intended to govern public oversight activities, even though special arrangements may be made in that respect. The possibility of restricting the safeguards provided by the GDPR does not however preclude its application.

105. Third, in the light of the general allocation of competences between the European Union and the Member States, public oversight activities do not appear to be reserved exclusively for the latter.

106. To take the specific example of parliamentary scrutiny, the two inquiries into the 'Dieselgate' affair, launched concomitantly by the European Parliament [36] and the German Bundestag (Parliament), demonstrate the overlapping competences in this area.

107. Admittedly, it could be argued that the scope of EU law covers only those monitoring activities that are relevant to the application of the provisions of that law.

108. Such an approach would, however, amount to reintroducing the concretising interpretation of the 'scope of Union law' and would therefore pose the same risks of legal uncertainty. Given the very nature of a parliamentary inquiry, which is designed to shed light on the circumstances of a case, it seems to me to be hard to predict whether there will be a specific link between the activities of a committee of inquiry and the application of provisions of EU law. [37]

109. In this context, consideration should be given to the objective of legal certainty pursued by the provisions of the GDPR, which seek to prevent fragmentation in the implementation of data protection across the European Union. [38]

110. In view of this objective, and in line with the solution adopted by the Court of Justice in *Österreichischer Rundfunk and Others*, [39] decided under Directive 95/46, the scope of the GDPR should be interpreted in such a way as to include public oversight activities, irrespective of the link they have with the application of specific provisions of EU law.

111. In the light of the foregoing, I propose that the answer to the first question referred for a preliminary ruling should be that the activities of a committee of inquiry set up by a Parliament of a Member State in the exercise of its right to scrutinise the executive fall within the scope of EU law within the meaning of the first sentence of Article 16(2) TFEU.

### *The second question*

112. By its second question, the referring court asks whether the activities of the committee of inquiry in the main proceedings come within the scope of the exception set out in Article 2(2)(a) of the GDPR, read in the light of recital 16 of that regulation, considering that the subject matter of its inquiry relates to matters of national security.

113. I do not believe that they do, for several reasons.

114. First, given the broad scope of the GDPR, the exception applied to activities concerning national security should be narrowly construed. I infer from this that only those activities whose immediate purpose is national security fall within this exception.

115. This is clearly not the case with the activities of the committee of inquiry in the main proceedings, which has been entrusted with the task of scrutinising federal government bodies.

[36] See Decision (EU) 2016/34 of the European Parliament of 17 December 2015 on setting up a Committee of Inquiry into emission measurements in the automotive sector, its powers, numerical strength and term of office (OJ 2016 L 10, p. 13).

[37] This raises the question of how to characterise the Austrian Parliament's inquiry into the 'Ibizagate' affair, concerning irregularities in the award of public contracts; the inquiry launched by the Belgian Senate in 1995 into organised crime in Belgium; or the ongoing investigation by the French National Assembly's committee of inquiry into 'the reasons for France's loss of sovereignty and energy independence'.

[38] See recitals 9 and 13 of the GDPR.

[39] Judgment of 20 May 2003 (C-465/00, C-138/01 and C-139/01, EU:C:2003:294, paragraphs 45 to 47).

116. Admittedly, to the extent that the scrutiny in question relates to the functioning of the BVT, whose task it is to ensure the integrity and continuity of State institutions, the committee's activity may have contributed *indirectly* to the safeguarding of national security.

117. However, such a contribution does not alter the nature of the activities entrusted to a committee of inquiry and cannot exclude them from the provisions of the GDPR. Otherwise, one might ask oneself whether an advertising agency hired by the Ministry of Defence to promote career opportunities in the army should not be similarly exempt.

118. Second, if the application of the GDPR were to depend on the subject matter of a parliamentary inquiry, this would be contrary to the objective of legal certainty pursued by the EU legislature.

119. Given its changing nature, the subject matter of a parliamentary inquiry does not provide a substantial enough basis for determining the scope of the GDPR. Circumstantial aspects, such as the implication of a defence minister in a corruption case – which might emerge (or be disproved) during the inquiry – cannot serve as a guide to that end.

120. Third, the interpretation of the exception contained in Article 2(2)(a) of the GDPR should take into account the *ratio legis* of that provision. This seems to me to be linked to the impossibility of reconciling certain fundamental aspects of the right to respect for personal data with the secrecy inherent in certain activities concerning national security.

121. As an illustration, I do not see how the domestic intelligence services could ensure respect for the rights to information and access, enshrined in Articles 14 and 15 of the GDPR, without compromising surveillance activities targeting persons suspected of belonging to a terrorist movement. In such a case, the requirements arising from the GDPR appear fundamentally incompatible with national security interests.

122. By contrast, it seems to me that the activity of a parliamentary committee of inquiry does not face any such insurmountable obstacle. Therefore, I do not see how complying with the obligations under the GDPR could jeopardise any contribution it might make towards safeguarding national security.

123. Evidently, the publicity that usually accompanies the activities of committees of inquiry is part of the *public* dimension of parliamentary scrutiny. The objective of transparency is, however, diametrically opposed to the *ratio legis* of Article 2(2)(a) of the GDPR, which seeks to protect secrets of national security.

124. Fourth, even if a properly conducted parliamentary inquiry may, in some cases, be incompatible with respect for GDPR requirements – for example, where the committee obtains access to confidential documents containing personal data – I would point out that Article 23(1)(a) and (h) of the GDPR provides for the possibility of restricting the rights and obligations laid down in Article 5, Articles 12 to 22 and Article 34 of that regulation, where such restriction is necessary to safeguard monitoring in the interests of national security.

125. It follows, in my view, that any connection that exists between the subject matter of a parliamentary inquiry and national security matters should not affect the obligation of the committee of inquiry to apply the GDPR. In view of the institutional context in which the activities of such committees – whose members participate in the work of the Parliament's

legislative bodies – take place, it seems relatively straightforward to make the necessary legislative adjustments in order to take into account the specific purpose of certain parliamentary inquiries, as provided for in Article 23(1) of the GDPR.

126. For all those reasons, I propose that the Court's answer to the second question should be that the activities of a parliamentary committee of inquiry investigating the activities of a police State-protection authority, that is to say, activities concerning the protection of national security within the meaning of recital 16 of the GDPR, do not come within the scope of the exception provided for in Article 2(2)(a) of that regulation.

### *The third question*

127. By its third question, the referring court asks whether the competence of a single supervisory authority, established pursuant to Article 51(1) of the GDPR, in respect of the complaints referred to in Article 77(1) of that regulation can arise directly from that provision, read in conjunction with Article 55(1) of the GDPR.

128. This question, which is raised in the event that the GDPR does apply to the activities of the committee of inquiry in the main proceedings, can be attributed to obstacles of a constitutional nature. In the opinion of the Verwaltungsgerichtshof (Supreme Administrative Court) and certain interested parties, the principle of the separation of powers specific to Austrian law precludes an administrative body – in this case, the Datenschutzbehörde – from interfering in the activities of the Parliament by investigating complaints about it.

129. The third question thus seeks to establish the scope of the direct effect of the combined provisions of Article 55(1) and Article 77(1) of the GDPR, where the competence of the single supervisory authority set up by a Member State is likely to be limited by a constitutional principle.

130. Since the GDPR is an EU regulation, it must be borne in mind that in principle it is directly applicable in its entirety, in accordance with the second paragraph of Article 288 TFEU, as confirmed by the second subparagraph of Article 99(2) of the GDPR. [40]

131. According to the case-law of the Court of Justice, the position is otherwise only where a regulatory provision necessitates the adoption of measures of application, in the light of the discretion enjoyed by the Member States in respect of its implementation. [41]

132. In that regard, I consider that the combined provisions of Article 77(1) of the GDPR, which provides for the competence of the supervisory authorities to examine the complaints referred to therein, and of Article 55(1) of that regulation are sufficiently clear and unconditional to be applied directly.

[40] See also judgment of 15 March 2017, *Al Chodor* (C-528/15, EU:C:2017:213, paragraph 27 and the case-law cited).

[41] See judgments of 11 January 2001, *Monte Arcosu* (C-403/98, EU:C:2001:6, paragraph 28), and of 14 April 2011, *Vlaamse Dierenartsenvereniging and Janssens* (C-42/10, C-45/10 and C-57/10, EU:C:2011:253, paragraph 48).

133. I would add that the Court of Justice has already confirmed the direct effect of Article 58(5) of the GDPR by holding that a national supervisory authority may rely on the capacity to initiate or engage in legal proceedings that is conferred on it by that provision in order to bring or continue a legal action against a private party, even in the absence of any legislative measure of application taken to that effect by the Member State concerned. [42]

134. Furthermore, in the circumstances of the case in the main proceedings, I do not consider that any additional measure of application is necessary to regulate the procedural arrangements for the complaint referred to in Article 77 of the GDPR. The Datenschutzbehörde regularly investigates such complaints, the only question being that of its competence in respect of parliamentary bodies.

135. However, that question has not been left to the discretion of the Member States.

136. Clearly, the effective exercise of the right to lodge a complaint presupposes the prior creation of one or more supervisory authorities, in accordance with Article 51(1) of the GDPR, which requires the intervention of the Member States. Yet that is a question of the direct effect of that provision, which does not arise in the main proceedings.

137. As for the number of supervisory authorities to be established under Article 51(1) of the GDPR, the institutional discretion left to the Member States in the matter cannot result in the powers of the single authority set up by the Austrian legislature being limited. The opposite interpretation would deprive Article 55(1) and Article 77(1) of the GDPR of their direct effect and risk weakening the effectiveness of all the other provisions of that regulation that may be the subject of a complaint.

138. Lastly, with regard to the obstacles of a constitutional nature that exist in Austrian law, they cannot justify a refusal to apply the provisions of the GDPR. According to the settled case-law of the Court, the effect of an EU measure cannot be affected by allegations that it runs counter to principles of a national constitutional structure. [43]

139. In answer to the third question, I propose therefore that the Court of Justice rule that, if a Member State has established only a single supervisory authority in accordance with Article 51(1) of the GDPR, the competence of that authority in respect of the complaints referred to in Article 77(1) of that regulation arises directly from that provision, read in conjunction with Article 55(1) of that regulation.

## Conclusion

140. Given all of the foregoing considerations, I propose that the Court should answer the questions referred by the Verwaltungsgerichtshof (Supreme Administrative Court, Austria) as follows:

(1) The activities of a committee of inquiry set up by a Parliament of a Member State in the exercise of its right to scrutinise the executive fall within the scope of EU law within the meaning of the first sentence of Article 16(2) TFEU; accordingly Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural

[42] Judgment of 15 June 2021, *Facebook Ireland and Others* (C-645/19, EU:C:2021:483, paragraph 113).

[43] Judgment of 17 December 1970, *Internationale Handelsgesellschaft* (11/70, EU:C:1970:114, paragraph 3).

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), applies to the processing of personal data by such a committee.

(2) The activities of a committee of inquiry which has been set up by a Parliament of a Member State in the exercise of its right to scrutinise the executive, and which is investigating the activities of a police State-protection authority, that is to say, activities concerning the protection of national security within the meaning of recital 16 of Regulation 2016/679, do not come within the scope of the exception provided for in Article 2(2)(a) of that regulation.

(3) If a Member State has established only a single supervisory authority in accordance with Article 51(1) of Regulation 2016/679, the competence of that authority in respect of the complaints referred to in Article 77(1) of that regulation arises directly from that provision, read in conjunction with Article 55(1) of that regulation.