

Case C-33/22 Österreichische Datenschutzbehörde confirms that the GDPR has general application to Member States' Parliaments

Dr Karen Mc Cullagh*

Case C-33/22 - *Österreichische Datenschutzbehörde*, Judgement of the Court of Justice of the European Union (Grand Chamber) of 16 January 2024 (ECLI:EU:C:2024:46)

Abstract

The CJEU was asked in a preliminary reference to consider the applicability of the GDPR to a member state parliamentary committee of inquiry set up to scrutinise the executive branch of government. The Grand Chamber ruled that its investigations and data processing actions are subject to the GDPR and concomitant supervisory mechanisms unless they fall under specific exemptions, such as national security or activities falling outside the scope of EU law.

Keywords: GDPR, data protection, material scope of application – parliament – national security exemption - supervisory authorities – competence – separation of powers.

I. The Facts

On 16th January 2024 the Court of Justice (henceforth: ECJ) issued, in C-33/22 *Österreichische Datenschutzbehörde v WK*,¹ its preliminary ruling on whether the personal data processing activities of a Parliament of a Member State fall within the scope of the General Data Protection Regulation 2016/679² (henceforth: GDPR) and if the national security exemption therein should be interpreted broadly or narrowly. It further ruled on whether provisions of the GDPR relating to the right of a data subject to lodge a complaint with a national supervisory authority are directly applicable, despite the constitutional principle of separation of powers.

The facts of this case concern the processing activities by a committee of inquiry established by the Chamber of Representatives of the Austrian Parliament to investigate allegations of the exertion of political influence on the Austrian Federal Office for the Protection of the Constitution and Counter Terrorism (henceforth: the BVT).³ The allegations included abuse of authority by BVT staff, wiretapping, 'alleged exploitations of investigations targeting certain extremist movements', and politically motivated appointments within the BVT.

An undercover investigator in the police intervention group responsible for combating street crime appeared as a witness before the committee of inquiry. His name (first and last) was included in the hearing minutes despite his request for anonymisation due to the nature of his job, on the basis that his identity had already been disclosed as the hearing was accessible by media representatives.

* Dr Karen Mc Cullagh is a Lecturer in Law at the University of East Anglia, UK. For Correspondence: k.mccullagh@uea.ac.uk; This commentary is based on an Op-ed that appeared in the EU Law Live blog. The author thanks Sarah König for answering queries on her article and the ECPRD surveys.

¹ C-33/22 *Österreichische Datenschutzbehörde*, [2024] ECLI:EU:C:2024:46.

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).

³ On 1 December 2021, the Directorate of State Protection and Intelligence Services succeeded that office.

The publication of his name prompted the witness to file a complaint with the Austrian Data Protection Authority under Article 77(1) GDPR, requesting a determination that the publication of his full name violated the GDPR. The national data protection supervisory authority (henceforth DPA) rejected the complaint on the ground of lack of competence. It asserted that the constitutional principle of separation of powers precluded it, as a part of the executive branch, from monitoring whether the committee of inquiry, which is a part of the legislature, complied with the GDPR.

The DPA's decision was appealed to the Federal Administrative Court, which annulled the DPA's decision. It subsequently reached the Supreme Administrative Court, which stayed proceedings and initiated a reference for a preliminary ruling by the ECJ.

I. The Preliminary Reference

The ECJ was asked to consider three inter-related questions. Firstly, whether a parliamentary committee of a Member State is obliged to comply with the GDPR when processing personal data. Secondly, whether a parliamentary committee can rely on the Art2(2)(a) national security exemption in respect of its processing activities. Thirdly, whether a national supervisory authority established by a Member State could have competence in relation to supervision of the parliamentary committee supervision notwithstanding the constitutional principle of separation of powers.

a. Applicability of the GDPR to Parliamentary activities

In answering the first question, the Court had to consider whether the GDPR applies to the activities of a Parliamentary committee of a Member State. The ECJ cited C-272/19 *VQ v Land Hessen*, a case in which the court ruled that a Member State Parliamentary committee that contributed indirectly to parliamentary activity was not, in principle, excluded from the scope of the GDPR.⁴ It made this determination on the basis that the status of the parliamentary body should not be a determining factor. Instead, the focus should be on whether it satisfies the Article 4(7) GDPR definition of a 'controller' as being the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Thus, it reasoned that a parliamentary committee which contributed only 'indirectly' to parliamentary activity could nevertheless be a data controller because it determined the purposes and means of processing of personal data.⁵

In the instant case, the Court cited *Land Hessen* in support of its reasoning that the status of the Committee of Inquiry, that is, a body whose activity is 'directly and exclusively parliamentary in nature' should not be a determining factor when deciding the applicability of the GDPR.⁶ Instead, it reasoned that when determining whether the GDPR is applicable, the focus should be on the category of activities of the controller's processing rather than the identity of the controller itself.⁷ As the Committee of Inquiry had responsibility for determining the purposes and means of processing of personal data it could be considered a controller within the scope of the GDPR.

b. Scope and Applicability of National Security Exemption

⁴ C-272/19 *VQ v Land Hessen*, Judgment of the Court (Third Chamber) of 9 July 2020, ECLI:EU:C:2020:535.

⁵ *VQ v Land Hessen*, (n 4) para 71.

⁶ *Österreichische Datenschutzbehörde v WK*, (n 1) para 40.

⁷ *Österreichische Datenschutzbehörde v WK*, (n 1) paras 38, and 41.

Having established the parliamentary committee could be considered a controller, the Court quickly turned its attention to the central issue in the case, namely whether the Art 2(2)(a) GDPR national security exemption applied to the Committee.

The Court had first considered the applicability of exemptions in *VQ v Land Hessen*. In that case, the court noted that the scope of the GDPR is broadly defined in Article 2 such that the exemptions in Article 2(2) must be interpreted restrictively. It reasoned that the fact that an activity is characteristic of the State or of a public authority is not sufficient ground for the EU's common foreign and security policy exemption in Art 2(2)(b) or Art 2(2)(d) 'Prevention, investigation, detection or prosecution of criminal penalties,' to automatically apply. It is instead necessary that the activity is one of those explicitly mentioned by that provision or that it can be classified in the same category. It ruled that while the activities of the Petitions Committee were incontestably public, and that committee contributed indirectly to the parliamentary activity, and are political as much as administrative, it was not clear from the case files that they correspond to those mentioned in Article 2(2)(b) and (d) GDPR or that they could be classified in their same category. The Court also noted that the GDPR does not contain, in recital 20 and in Article 23, a specific exemption in respect of parliamentary activities.⁸

In the instant case, the Court considered the applicability of the Article 2(2)(a) "acting outside the scope of Union law" exemption. It did not explain what that would entail but referred instead to the national security example outlined in Recital 16 GDPR. In line with the AG's Opinion, which argued for the national security exception to be interpreted narrowly,⁹ the Court recalled C-439/19 *Latvijas Republikas Saeima*¹⁰ and C-306/21 *Koalitsia 'Demokratichna Bulgaria – Obedinenie'*¹¹ in support of its reasoning that the Art 2(2)(a) GDPR exemption must be interpreted restrictively, such that it would encompass those activities that are 'intended to protect essential State functions and the fundamental interests of society' and not automatically apply in respect of an activity of a parliamentary committee established to scrutinise the executive.¹² It also referred to C-742/19 *Ministrstvo za obrambo* in support of its determination that although it is for Member States, in accordance with Article 4(2) TEU to define their essential security interests, the activities of a committee set up to investigate allegations of political influence could not automatically be regarded as activities concerning national security and exempt from the GDPR.¹³

c. Competence of the National Data Protection Authority

The final question considered by the ECJ was whether a Member State supervisory authority has competence to hear complaints relating to the processing of personal data by a committee of inquiry established by a Member State parliament. At issue was whether the principle of the separation of powers precludes an administrative body – in this case, the Datenschutzbehörde (DPA) – from interfering in the activities of the Parliament – a legislative body - by investigating complaints about it.

This question required the Court to establish the scope of the direct effect of the combined provisions of Article 55(1) (competence of supervisory authority) and

⁸ *VQ v Land Hessen*, (n 4) para 72.

⁹ Opinion of Advocate General Szpunar, in Case C-33/22 *Österreichische Datenschutzbehörde* other parties: WK, Präsident des Nationalrates, delivered on 11 May 2023.

¹⁰ Case C-439/19, *Latvijas Republikas Saeima*, ECLI:EU:C:2021:504

¹¹ C-306/21, *Koalitsia 'Demokratichna Bulgaria – Obedinenie'*, ECLI:EU:C:2022:813.

¹² *Österreichische Datenschutzbehörde v WK*, (n 1) para 43

¹³ *Ibid*, paras 50-52.

Article 77(1) right to lodge a complaint with a supervisory authority) of the GDPR, where the competence of the single supervisory authority set up by a Member State is likely to be limited by the constitutional principle of separation of powers. The court reasoned, referring to the principle of Direct Effect in EU Law that Articles 77(1) and 55(1) are sufficiently clear for their implementation to have direct effect. Therefore, where a Member State chooses to establish a DPA, that DPA has all the powers granted to it by the GDPR.

It further noted that Article 55(3) GDPR provides that DPA's are not competent to supervise processing operations of courts in their judicial capacity¹⁴ but interpreted its silence regarding parliaments as conferring competence on the DPA authority to monitor compliance by the parliamentary committee with the GDPR, notwithstanding the principle of separation of powers, thereby underscoring the direct effect and primacy of EU law, including the GDPR, over national constitutional law. The Court also noted that Article 51(1) of the GDPR grants each Member State a margin of discretion which empowers it to establish however many supervisory authorities as it considers necessary in accordance with its constitutional arrangements. It ruled that where a Member State has chosen to establish a single supervisory authority but has not explicitly conferred on it the power to oversee executive committees, including parliamentary committees of inquiry, it will be deemed have competence to do so.

Commentary

Personal data is routinely processed in EU Member State parliaments in a variety of activities e.g., when responding to oral and written questions, during debates, hearings, and inquiries. However, when the GDPR first came into force on 25th May 2018 there was uncertainty regarding its application to Parliamentary activities, and if so, whether the exemptions therein should be interpreted narrowly or broadly. The applicability of data protection laws to parliamentary activities was not however a new issue. In this regard, Lazarakos observed that “the issue of the applicability of data protection legislation to core parliamentary activities has existed as long as data protection.”¹⁵ The continuing uncertainty was captured in a survey conducted by the European Centre for Parliamentary Research and Documentation (ECPRD) of 40 parliamentary chambers shortly after the GDPR entered into force. In the survey, 67% of parliamentary chambers considered the GDPR to apply directly or indirectly via Member State laws to their activities, whilst 21% did not and the remainder were undecided. For instance, Ireland was undecided whilst Denmark expressly exempted the activities of its Parliament from the scope of its data protection law, and Austria provided a specific exemption for core parliamentary activities in its data protection law.¹⁶ Furthermore, there was a lack of clarity regarding whether a national supervisory authority has the competence to monitor compliance with the GDPR by a parliamentary committee, which is a part of the legislature, or is precluded from doing so by the principle of separation of powers because supervisory authorities are part of the executive. Indeed, the same ECPRD survey also found that some parliamentary chambers considered themselves to be subject to their respective national supervisory

¹⁴ Ibid, para 66.

¹⁵ Grigoris Lazarakos, “Parliamentary activity and the General Data Protection Regulation (GDPR): The Paradigm of the Hellenic Parliament,” (2021) 1 *International Journal of Parliamentary Studies*, 315–326

¹⁶ The ECPRD surveys were administered by the Austrian Parliament’s correspondent’s office; Sarah König, “The GDPR’s Application and Supervisory Authorities’ Remit on National Parliaments’ Data Processing in Parliamentary Core Activities,” (2022) 2 *International Journal of Parliamentary Studies*, 99–109, 102.

authority's remit whilst others claimed not to be because of the constitutional principle of separation of powers.¹⁷

As outlined above, the ECJ first considered whether the activities of a Parliamentary Petitions Committee fell within the concept of 'controller' in the GDPR in *C-272/19 VQ v Land Hessen*. In that case it ruled that the reference to a "public authority" within the definition of "controller" in Article 4(7) GDPR could include the Petitions Committee of the State Parliament.¹⁸ It further ruled that the processing of personal data carried out by the Petitions Committee of the Parliament of Land Hessen is subject to the GDPR in so far as the Committee determines, alone or with others, the purposes and means of the processing.

For many scholars and practitioners, the ruling was unsurprising since it accorded with previous jurisprudence and the approach adopted in their national data protection laws. For scholars such as Heberlein the ruling confirmed the general application of the GDPR to personal data processing activities by parliamentary committees¹⁹ and Aertgeerts similarly formed the view that "with regard to the scope of the GDPR, there is little to criticize in the Court's judgment,"²⁰ whilst practitioners such as Knight observed that the judgment reflected the position in their national data protection laws – in the case of the UK, (which was an EU Member State at the time the *Land Hessen* ruling was delivered), the Data Protection Act 2018 does not contain an exemption for Parliamentary processing activities.²¹

Yet, other scholars were not so certain about the application of the GDPR to activities of parliamentary committees following the *NQ v Land Hessen* ruling. Their uncertainty stemmed from the Court describing the activities of the Parliamentary Committee as 'political as much as administrative' and that they only 'indirectly' contribute to parliamentary activity.²² Indeed, this description prompted Posnik to query whether the Court would, in a future case, view an activity that is 'directly' part of parliamentary activity (i.e., law-making) as a 'characteristic activity of the State' and classify it in the same category as Article 2(2)(a), (b) or (d) GDPR.²³ König likewise opined that the decision revealed "a need for a differentiated assessment of data processing activities given the distinctive criteria of indirect and direct contributions to parliamentary procedure as well as those activities that are aimed at protecting essential State functions and the fundamental interests of society."²⁴ It was therefore inevitable that when the ECPRD survey was repeated after the *Land Hessen* judgment a uniform approach regarding application of the GDPR to Parliamentary activity was not apparent. Indeed, of the 7 Parliamentary Chambers that indicated a change of stance, 3 had changed their position from non-application to that of application and 2 changed

¹⁷ *Ibid*, 101.

¹⁸ *VQ v Land Hessen* (n 4), para 73.

¹⁹ Horst Heberlein, "Bereichsausnahme für Parlamente? Geltung der DSGVO für parlamentarische Tätigkeiten," (2021) 2 *Zeitschrift für Datenschutz*, 85–88.

²⁰ Pieter Aertgeerts, 'Judicial independence meets data protection: de onafhankelijkheid van rechterlijke instanties onder de prejudiciële verwijzingsprocedure en de werkingssfeer van de Algemene Verordening Gegevensbescherming (noot bij HvJ 9 juli 2020, nr. C-272/19, ECLI:EU:C:2020:535, *Land Hessen*)' (2020) *Tijdschrift voor Bestuurswetenschappen en Publiekrecht* (10), 543-546.

²¹ The Data Protection Act 2018, Schedule 2, para 13 includes a broad exemption from data subject rights where compliance would infringe Parliamentary privilege; Christopher Knight, "Parliaments and the GDPR," *Panopticon Blog*, (10 July 2020), <<https://panopticonblog.com/2020/07/10/parliaments-and-the-gdpr/>>, At that time the UK was an EU Member State.

²² *VQ v Land Hessen*, (n 4) para 71.

²³ Rosi Posnik, "Legal Considerations on the CJEU Judgement of 9 July 2020, C-272/19," (2021) 1, *International Journal of Parliamentary Studies*, 154-159, 159.

²⁴ König, (n 16) 106.

the status of the GDPR from provisional to application, yet 2 had declared parliamentary activities as being exempt from the application of the GDPR.²⁵

There was a concomitant lack of clarity regarding whether a national supervisory authority has competence to monitor whether a parliamentary committee, which is a part of the legislature, is subject to the GDPR or exempt because of the principle of separation of powers on the basis that supervisory authorities are part of the executive. Posnik contended that the matter was not settled because “The fact that parliamentary activities are not explicitly mentioned in recital 20 or in Article 55 GDPR, does not necessarily mean that the GDPR applies to them: If they are not covered by the scope of the Regulation itself, an exception in Article 55 GDPR or recital 20 is not necessary. In any case, from the perspective of the separation of powers, the control of legislative bodies by an administrative authority would be no less problematic than the control of the judiciary.”²⁶ Predictably, the ECPRD survey conducted in 2021 reported continuing disparity of approach. Of those Parliaments that responded, 60% were subject to their respective national supervisory authority’s remit. By contrast, 24% were not. Also, none had established a specialist supervisory authority.²⁷

The disparity of approach was problematic because recital 10 of the GDPR provides that “consistent and homogenous application of the rules for the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data should be ensured throughout the Union,” yet the effect of *NQ v Land Hessen* was that data subjects could have rights and remedies in respect of personal data processed by parliaments in some Member States but not in others.

Accordingly, the *Österreichische Datenschutzbehörde* preliminary reference provided a valuable opportunity to revisit the issues and, in particular, to obtain clarification on the applicability of the GDPR and exemptions therein to the personal data processing activities of parliaments in Member State and to confirm whether they are subject to the supervision of a national data protection regulator. The Court seized the opportunity. Following the preliminary ruling in *Österreichische Datenschutzbehörde* it is now clear that the personal data processing activities of a Parliament of a Member State generally fall within the scope of the GDPR. It definitively confirms that the Court does not distinguish between legislative and executive activities when considering whether the GDPR applies to Parliamentary activities. Instead, the presumption is that the GDPR applies to all personal data processing, unless one of the exemptions specified in Article 2(2) applies. Moreover, when considering whether the Art 2(2)(a) national security exemption may be applicable, it should be interpreted narrowly. The Court also confirmed that provisions of the GDPR relating to the right to lodge a complaint with a national supervisory authority apply directly. Accordingly, all Member States must now accept an obligation for their parliamentary bodies to comply with the GDPR and take practical steps to ensure that complaints in respect of the personal data processing activities by their parliamentary bodies are subject to supervision by either a national data protection regulator, or specialist regulator, if that better fits their national constitutional framework.

Concluding remarks

The lingering doubt regarding the application of the GDPR to the personal data processing activities of parliamentary bodies in EU Member States since it came into force on 25th May 2018 has now been resolved. It does, save when an exemption in

²⁵ König, (n 16) 104.

²⁶ Posnik, (n 24) 159.

²⁷ König, (n 16) 102.

Art 2(2) is applicable. The clarity this preliminary ruling brings is to be welcomed because it will lead to greater harmonisation of data protection laws in Member States and, in practical terms, it will result in data subjects having equal data protection rights in respect of personal data processed by Parliamentary bodies in all Member States. Relatedly, they will be able to lodge data protection complaints before their national supervisory authority or specialist regulator.