EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

SECOND SECTION

DECISION

Application no. 35473/23
Janne Cecilie THORENFELDT
against Norway

The European Court of Human Rights (Second Section), sitting on 10 March 2026 as a Chamber composed of:

Jovan Ilievski*, President*,
Arnfinn Bårdsen,
Péter Paczolay,
Oddný Mjöll Arnardóttir,
Gediminas Sagatys,
Stéphane Pisani,
Juha Lavapuro*, judges*,

and Andrea Tamietti, *Section Registrar,*

Having regard to the above application lodged on 18 September 2023,

Having regard to the decision to give notice to the Norwegian Government of the complaints under Articles 8 and 13 of the Convention and to declare the remainder of the application inadmissible,

Having regard to the observations submitted by the respondent Government and the observations in reply submitted by the applicant,

Having deliberated, decides as follows:

THE FACTS

1. The case concerns the applicant's complaint that a national labour and welfare institution had failed to sufficiently protect the confidentiality of records containing her personal information and health data. The applicant had been both an employee and a service user of the institution in question and invokes Articles 8 and 13 of the Convention.

2. The applicant, Ms Janne Cecilie Thorenfeldt, is a Norwegian national, who was born in 1969 and lives in Oslo. She was represented before the Court by Mr M. Andenas, a lawyer practising in Oslo.

3. The Norwegian Government ("the Government") were represented by their co-Agent, Ms K. Bjelland, of the Office of the Attorney General for Civil Affairs, assisted by Mr Stein-Erik Jahr Dahl, an advocate at the same office.

4. The facts of the case, as submitted by the parties, may be summarised as follows.

A. Background to the case

5. The Norwegian Labour and Welfare Administration (NAV) manages around one-third of the national budget through its administration of, *inter alia*, unemployment benefits, sickness benefits, retirement pensions, child benefits and cash-for-care benefits. The NAV thus processes vast quantities of personal data relating to millions of Norwegians. It is subordinate to the Labour and Welfare Directorate and has approximately 19,000 employees, 14,000 of whom are employed at national level, with the rest employed at local level.

6. The applicant was employed by the NAV from 2007 onwards and was based in its Nordstrand office. After an accident in 2015 she was granted a work assessment allowance in December 2016 and consequently became a service user of the NAV. For the whole period relevant to the present case, the applicant's social benefit claims were not processed by her local office, but by other offices. The Nordstrand office's role, in so far as the applicant was concerned, was mainly to make sure that incoming mail and tasks concerning her claims were forwarded to the correct office. That role was carried out by a limited number of trusted employees, who were not part of the management team and who did not represent the NAV as an employer *vis-à-vis* the applicant.

7. In 2018 the applicant suspected that some of her colleagues had had unauthorised access to her case file, which contained her personal information and health data. Therefore, on 15 and 31 May 2018 she sought information from the NAV about who had accessed her case file. She received a copy of an activity log which showed the dates on which her file had been accessed and the office involved, but no specific information about who had accessed it or why. On 22 June 2018 the applicant requested comprehensive follow-up information and the NAV replied to this request on 24 October 2018.

B. Investigation by the Data Protection Authority

8. In 2018 the applicant contacted the Data Protection Authority about the matter. The Data Protection Authority initiated an investigation and asked the NAV for a statement on data protection in relation to the employee data contained in its systems. Specifically, the Data Protection Authority asked the

NAV to submit a statement on how it handled its employees' personal data and their requests for access to information. The NAV sent its statement to the Data Protection Authority on 14 December 2018.

9. On 7 June 2019 the Data Protection Authority concluded that the NAV had not taken sufficient steps to determine the level of security required to protect its employees' personal data, an omission which had rendered unsatisfactory the security measures and technical solutions then in place. The Data Protection Authority considered this a breach of Article 32 of the General Data Protection Regulation (hereinafter "the GDPR" – see paragraph 25 below) taken in conjunction with Article 5 (1) (f), and the NAV was ordered to put in place suitable security arrangements to ensure its employees' privacy. The breach specifically concerned the following: (i) access control procedures in respect of the personal data of employees and their family members were "fragmented" and not consistently implemented throughout all NAV units; (ii) the data protection scheme for employee data was based on individual assessments of the relevant employee's needs; and (iii) the procedures for assigning a case to another office were not uniform across all NAV units. The Data Protection Authority also recommended that the NAV further consider whether employees should have access to information about colleagues in the same unit.

10. On 13 September 2019 the NAV replied to the Data Protection Authority, agreeing that technical solutions had been lacking when it came to its employees' personal data, and it presented a plan incorporating measures to resolve such issues which would be implemented on 1 January 2020.

11. On the basis of the NAV's response, the Data Protection Authority found that the breach had been remedied. The case was therefore closed on 21 January 2020.

C. Proceedings before the domestic courts

12. On 25 March 2020 the applicant again requested information about who had accessed her file. She obtained a copy of another activity log, in respect of which she sought clarification as to why several persons had accessed her file. She requested additional information on 17 April, 3 June and 4 December 2020. The NAV gave a collective response to all of the applicant's requests on 11 January 2021. It specified that its data protection unit had investigated instances of her file being viewed by approximately 45 different people, and an account was given of what the unit had found in each case.

13. In 2021 the applicant brought an action against the NAV in the Oslo District Court (*tingrett*), seeking to obtain a declaratory judgment finding a violation of her rights under the relevant data protection legislation, including Articles 12 and 15 of the GDPR (see paragraph 25 below). She also lodged a claim in respect of non-pecuniary damage (without specifying the amount

claimed), alleging that her colleagues in the NAV had had unauthorised access to her case file, which contained personal health data, and that as a result she had suffered emotional distress. She referred to the right to privacy only briefly in an opening section of the writ of summons.

14. On 18 January 2022 the Oslo District Court dismissed the action for a declaratory judgment, finding in favour of the State of Norway.

15. By a letter dated 18 February 2022, the applicant appealed against the judgment to the Borgarting Court of Appeal (*lagmannsrett*). From 17 until 20 January 2023 the court held an oral hearing, where the statements of nine witnesses were heard.

16. On 2 March 2023 the Court of Appeal found in favour of the State of Norway. It dismissed both the action for a declaratory judgment and the claim for damages. No costs were awarded for any of the court proceedings. The court first of all concurred with the Data Protection Authority's assessment and conclusion that the NAV's procedures for protecting service-user data belonging to the organisation's own employees had not been in compliance with Article 32 of the GDPR taken in conjunction with Article 5 (1) (f) (see paragraph 9 above). The Court of Appeal therefore found that the NAV, prior to the implementation of the new measures in 2020, had never implemented sufficient technical and organisational measures to ensure that its employees' personal data were protected. This meant that employees could have access to service-user information about colleagues in their own unit. Even after 2020 there might have been some "holes" in the procedures for processing service-user information concerning the organisation's own employees, but there were no indications that such "holes" had existed in respect of the applicant's benefit claims.

17. Concerning the 2018 information requests (see paragraph 7 above), the Court of Appeal noted that requests made by the applicant on 15 and 31 May had received replies from the NAV on 8 and 18 June 2018 respectively, thus within the time-limit provided for by section 16(1) of the Personal Data Act. As to the applicant's comprehensive request for follow-up information (see paragraph 7 above), the court noted that a new time-limit would normally begin to run if new information was requested. The assumption was therefore that a new time-limit had begun to run from 22 June 2018, pursuant to section 16 of the Personal Data Act. As the 2018 requests had been made before the GDPR had entered into force, the time-limit established by Article 15 § 3 of the GDPR had not applied. The court found that although the NAV's failure to give a provisional reply to the requests had constituted a breach of section 16(2) of the Personal Data Act, its responses had complied with the transparency requirements of Article 12 § 1 of the GDPR. Indeed, no aspects of the NAV's handling of the requests indicated that it had not fulfilled its obligation to facilitate the applicant's opportunity to exercise her rights under the GDPR. The NAV's responses had also met the information requirements under the right of access provided for in

Article 15 § 1 (a)-(c) of the GDPR. The court did not accept that the rules concerning access had been breached, given that the NAV had provided access to all existing and available information.

18. As to the 2020 information requests (see paragraph 12 above), the Court of Appeal noted that the applicant's requests of 25 March, 17 April, 3 June and 4 December 2020 had all received responses from the NAV well within the time-limit of one month. As for the requests for more information on selected entries in the activity log, the NAV's initial response had been to inform the applicant that it had started looking into the matter and would get back to her with more information. As information about the purpose behind each viewing of her file had not been readily available in the administrative system, manual investigations into each instance had had to be carried out. Where the requested information had been available, the applicant had received it on the same day she had made her request. On the basis of an overall assessment, the Court of Appeal concluded that the NAV had not breached the time-limits provided for in Article 12 § 3 of the GDPR. It had responded to the requests for activity logs by providing copies of them to the applicant on the same day the requests had been made. It had also responded to requests for additional information on selected entries without undue delay, informing the applicant that investigations had been initiated in respect of the requests. Although the NAV's investigations into those specific log entries had each lasted between one month and nine months, this did not constitute a breach of the GDPR. As it had done in respect of the 2018 requests for activity logs (see paragraph 17 above), the Court of Appeal found, in respect of the 2020 requests, that the NAV's responses had complied with the transparency requirements of Article 12 § 1 of the GDPR and the information requirements of Article 15 § 1 (a)-(c), and no aspects of its handling of the requests indicated that it had not fulfilled its obligation to facilitate the applicant's opportunity to exercise her rights under the GDPR.

19. As to whether the applicant had suffered material or non-material damage as a result of the breach of Article 32 of the GDPR taken in conjunction with Article 5 (1) (f), the Court of Appeal held that it had been established that the concept of damage, within the meaning of Article 82 of the GDPR, should be interpreted broadly. In the applicant's case, the Court of Appeal nevertheless found that it had not been substantiated that she had suffered damage as a result of the breaches found. The court did not rule out the possibility that the strain the applicant had experienced as a result of her suspicions regarding unauthorised access to her personal data could have exceeded the threshold for non-material damage within the meaning of the GDPR. However, it could not see any causal link between that damage and the breaches of the GDPR. The court found no basis to conclude that the applicant's superiors or other colleagues had consciously abused her personal data or "snooped" ("*snoket*") on her by accessing those data with unprofessional or illegitimate aims. The breaches found by the court had

pointed to general flaws in the NAV's procedures, which had affected the applicant to the same extent as other service users. Those procedures had been changed in 2020, in response to an order issued by the Data Protection Authority (see paragraph 10 above). Accordingly, the Court of Appeal did not find it substantiated that the applicant had suffered damage as a result of the breach of Article 32 of the GDPR taken in conjunction with Article 5 (1) (f). It also concluded that it did not seem reasonable to make an award for damages under section 30 of the Personal Data Act (see paragraph 26 below).

20. By a letter dated 31 March 2023, the applicant appealed against the judgment to the Supreme Court (*Høyesterett*). She referred to the right to privacy only briefly in her appeal to the Supreme Court.

21. On 24 May 2023 the Supreme Court of Norway refused the applicant leave to appeal.

RELEVANT LEGAL FRAMEWORK

A. The Constitution

22. Article 92 of the Norwegian Constitution requires the authorities of the State to:

> "respect and ensure human rights as they are expressed in this Constitution and in the treaties concerning human rights that are binding for Norway."

23. Article 102 of the Constitution provides:

> "Everyone has the right to the respect for his or her privacy and family life, home and communications ..."

B. The Human Rights Act

24. The Convention is incorporated into Norwegian law through section 2 of the Human Rights Act. Section 3 of the Act provides:

> "The provisions of [the Convention] ... shall take precedence over any other legislative provisions that conflict with them."

C. The GDPR

25. The GDPR is incorporated into Norwegian law through section 1 of the Personal Data Act (*personopplysningsloven*, 2018). Section 2 of the EEA Act (*EØS-loven*) gives the GDPR precedence over other provisions in Norwegian law that govern the same matter (for cases concerning the GDPR, see, for example, *Biancardi v. Italy*, no. 77419/16, 25 November 2021).

D. The Personal Data Act

26. The Personal Data Act contains a separate provision on compensation in respect of non-pecuniary damage, which reads as follows:

Section 30 – Damages for non-pecuniary loss

> "A party who is liable to pay compensation pursuant to the rules in Article 82 of the General Data Protection Regulation can also be ordered to pay such damages for non-pecuniary loss as seems reasonable."

E. The Public Administration Act

27. Section 13 of the Public Administration Act (*forvaltningsloven*) provides the following:

> "It is the duty of any person providing services to, or working for, an administrative agency to prevent others from gaining access to, or obtaining knowledge of, any matter disclosed to him or her in the course of his or her duties concerning
>
> 1. an individual's personal affairs; or
>
> 2. technical devices and procedures ...
>
> The term 'personal affairs' shall not include [a person's] place of birth, date of birth, national registration number, nationality, marital status, occupation or place of residence or employment, unless such information discloses a client relationship or other matters that must be considered personal ...
>
> The duty of secrecy shall continue to apply after the person concerned has terminated his or her service or work ..."

COMPLAINTS

28. The applicant complained, under Article 8 of the Convention, of a violation of her right to respect for her private life owing to the insufficient protection of the confidentiality of her records at the NAV.

29. The applicant complained under Article 13 of the Convention that she had had no effective domestic remedy at her disposal in respect of the breach of her right to privacy.

THE LAW

A. Complaint under Article 8 of the Convention

30. The applicant considers that her records at the NAV were insufficiently protected and that as a consequence her right to respect for her private life was violated.

She invoked Article 8 of the Convention, which reads as follows:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

31. The Government objected to the admissibility of the case, noting that the applicant had failed to exhaust the available domestic remedies, as required by Article 35 of the Convention. They noted that the applicant had never relied on Article 8 of the Convention in the national courts, instead relying solely on the provisions of the GDPR throughout the domestic proceedings. The right to privacy had only briefly been referred to by the applicant in an opening section of the writ of summons and in the appeal to the Supreme Court (see paragraphs 13 and 20 above).

32. The applicant noted that Article 8 of the Convention had been mentioned several times in the domestic proceedings and that a complaint under the GDPR should, for the purposes of applying Article 35 of the Convention, be considered "in substance" a complaint under Article 8 of the Convention.

33. The general principles concerning exhaustion of domestic remedies are summarised in *Communauté genevoise d'action syndicale (CGAS) v. Switzerland* [GC], no. 21881/20, §§ 138-145, 27 November 2023. The Court notes that, according to established case-law concerning Norwegian cases, raising a Convention complaint only on appeal to the Supreme Court cannot in the Norwegian system normally be viewed as sufficient exhaustion of remedies in cases where nothing has prevented the applicant from raising the complaint before the lower courts. This consideration is supported by the provisions of the Dispute Act, from which it appears not only that appeals to the Supreme Court must normally target "errors" in the High Court's judgments, but also that the Supreme Court can normally only take on cases of general or particular importance. It follows that it is essentially inconsistent with the domestic civil procedural system and the role that the Supreme Court plays therein for an applicant to raise a Convention complaint for the first time before the Supreme Court. It follows also that an applicant cannot expect a complaint raised for the first time at that level of appellate jurisdiction to be decided on the merits (see *S.R. v. Norway* (dec.), no. 43927/17, § 31, 21 April 2020).

34. Moreover, the Court is not convinced by the applicant's argument that the action she brought under the GDPR can be seen as raising in substance a Convention complaint under Article 8 of the Convention (see paragraph 32 above). There is thus at least a serious doubt as to whether the applicant had exhausted domestic remedies the manner required by Article 35 of the

Convention. Even assuming that she had, the application is inadmissible for the reasons set out below.

35. The Court notes that the Government submitted also other objections as to the admissibility of the case, namely the lack of "significant disadvantage" and a victim status. In this respect either, the Court does not consider it necessary to examine these Government's objections.

36. The Government explained in their observations that, in the present case, as the preventive measures of access checks and activity logs had been in place at the relevant time, the applicant's personal data should be regarded as having been sufficiently protected. The activity log had shown all enquiries pertaining to case documents, by whom an enquiry had been made, and to which case handling system it had related. The comprehensive logs, coupled with the technical access checks, had enabled the NAV's data protection unit to investigate the historical processing of data by the individuals of whom the applicant had been suspicious. This had been done both before the domestic hearing and during the proceedings, as the applicant had continued to accuse new individuals of accessing her files without a work-related justification. The investigations had confirmed that the employees whose names appeared in the logs and who had had the relevant access had been involved in processing the applicant's benefit claims, thereby explaining why they had accessed the case documents in question. The evidence presented to the domestic courts had further proved that the NAV, as an employer, had not had access to the applicant's medical files. Moreover, there was no evidential basis in the activity logs or elsewhere to support a finding that any of the four colleagues in the NAV's Nordstrand office who had had the relevant access had been "snooping around" in the applicant's case file.

37. In addition, the Government explained that there had been additional safeguards in place which had further enhanced the protection of the applicant's case file. Firstly, the NAV had set out specific, written guidelines for registering and forwarding mail and tasks pertaining to social benefit claims from its own employees. It had also written guidelines with examples of what would amount to unlawful use of the technical access rights. Secondly, there had been written instructions for action to be taken against anyone who breached the prohibition against unauthorised access, with the punishments ranging from a written warning (as a minimum) to immediate termination of the relevant employment contract without notice. Thirdly, the NAV employees who had needed to access the applicant's case file to perform their tasks had been granted access to the relevant case handling systems only. Fourthly, the information in question had been protected by a statutory confidentiality obligation of unlimited duration, any breach of which would be punished by up to three years' imprisonment. Lastly, the NAV had created a separate unit – the NAV data protection unit – for the purpose of, *inter alia*, investigating any allegations of unlawful access to

personal data. The totality of those measures had provided a sufficient level of protection to meet the requirements under Article 8.

38. The applicant submitted that her rights under Article 8 of the Convention had been breached by the Government's deliberate choice to forward complaints and correspondence relating to social benefit claims by NAV employees from the local offices in which those individuals worked to other offices. That practice had meant that an excessive number of colleagues had had access to the health information of the employees in question, a state of affairs which had constituted an infringement of the right to private life under Article 8 of the Convention. The evidence confirming the existence of the unnecessary practice of widespread disclosure and dissemination of health information was solid.

39. The Court of Appeal and the Government had made too much of any evidential uncertainty concerning the applicant's allegation that, without justification, her immediate colleagues had accessed and read the health records attached to her social benefit claims. In this regard, it was important to bear in mind that proving that allegation was not decisive for whether a breach of Article 8 of the Convention had occurred. Maliciously accessing the applicant's health information without justification – a conduct in which her immediate colleagues and managers had engaged – constituted an aggravating factor and only added to the severity of the breach by the agents of the Government. Any uncertainty around the applicant's allegation concerning that conduct did not call into question the existence of the breach relating to the systemic deficiencies at issue, or diminish its gravity.

40. The Court notes that the NAV is a public institution for whose acts the State is responsible for the purposes of the Convention (see, *mutatis mutandis*, *Glass v. the United Kingdom*, no. 61827/00, § 71, ECHR 2004-II). The processing of information relating to an individual's private life comes within the scope of Article 8 § 1 of the Convention (see *Y.G. v. Russia*, no. 8647/12, § 33, 30 August 2022). Personal information relating to one's welfare benefits undoubtedly belongs to his or her private life. Article 8 of the Convention is therefore applicable in the present case. Indeed, this has not been contested by the parties.

41. Although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in effective respect for private or family life (see *Airey v. Ireland*, 9 October 1979, § 32, Series A no. 32). These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves (see *X and Y v. the Netherlands*, 26 March 1985, § 23, Series A no. 91, and *Odièvre v. France* [GC], no. 42326/98, § 40, ECHR 2003-III). In the present case, the parties agreed that Article 8 was applicable under its positive obligation aspect.

42. Information concerning an individual's health constitutes a key element of private life (see *L.H. v. Latvia*, no. 52019/07, § 56, 29 April 2014; *Y.Y. v. Russia*, no. 40378/06, § 38, 23 February 2016; and *Frâncu v. Romania*, no. 69356/13, § 52, 13 October 2020). Respect for the confidentiality of this information is crucial, not only to respect the sense of privacy of a patient, but also to preserve his or her confidence in the medical profession and in the health services in general. The disclosure of such data may dramatically affect his or her private and family life, as well as social and employment situation, by exposing him or her to opprobrium and the risk of ostracism (see *Z v. Finland*, 25 February 1997, § 96, *Reports of Judgments and Decisions* 1997-I; *P. and S. v. Poland*, no. 57375/08, § 128, 30 October 2012; and *Y.G. v. Russia*, cited above, § 45). The Court is of the opinion that similar considerations also apply when, as in the present case, the medical information is linked to the receipt of welfare benefits. The interest in protecting the confidentiality of such information will therefore weigh heavily in the balance when determining whether a State has fulfilled its positive obligation.

43. In the present case, the applicant submitted that some of her colleagues at the NAV had had unauthorised access to the file containing her personal information and health data, and that there had therefore been disclosure and dissemination of her health information by the NAV between 2016 and 2021.

44. The Court notes that, as a result of the Data Protection Authority's assessment and conclusions of 7 June 2019, new technical solutions protecting employees' personal data were introduced by the NAV on 1 January 2020 (see paragraphs 9 and 10 above). Accordingly, the Court will firstly examine the situation before 1 January 2020 and then the period thereafter.

45. The Court notes that, as regards the period before 1 January 2020, the NAV accepted that technical solutions had been lacking when it came to the protection of its employees' personal data (see paragraph 10 above). Similarly, in its judgment of 2 March 2023, the Court of Appeal concurred with the Data Protection Authority's assessment and conclusion that the NAV's procedures for protecting service-user data belonging to the organisation's own employees had not been in compliance with Article 32 of the GDPR taken in conjunction with Article 5 (1) (f) (see paragraph 16 above). The court therefore found that the NAV, prior to the implementation of the new measures in 2020, had never implemented sufficient technical and organisational measures to ensure that its employees' personal data were protected, meaning that employees could have access to service-user information about colleagues in their own unit. The Court has no reason to conclude otherwise.

46. As a result of the technical changes made in 2020, the previous system was extensively modified. With the changes, the NAV implemented both

preventive measures and measures that allowed it to retroactively clarify the activity in employees' case files, even including the period before 1 January 2020. Following the changes, as explained by the Government in their observations (see paragraphs 36 and 37 above), activity logs showed all enquiries pertaining to case documents throughout the whole period relevant to the applicant's complaint from the time she became service user of the NAV (see paragraph 6 above), by whom an enquiry had been made and to which case handling system it related. Employees were not granted access rights to all systems, but to only those case handling systems that they needed to access in order to carry out their tasks. Moreover, there were written guidelines with examples of what would amount to unlawful use of the technical access rights, and action would be taken against anyone who breached the prohibition against unauthorised access, with the punishments ranging from a written warning to immediate termination of the relevant employment contract without notice. The information was also protected by a statutory confidentiality obligation of unlimited duration, any breach of which would be punished by up to three years' imprisonment. In addition, a separate NAV unit – the NAV data protection unit – was created for the purpose of, *inter alia*, investigating any allegations of unlawful access. The Court notes that the applicant did not challenge the Government's allegations in these respects.

47. The Court notes in this connection that the present case differs fundamentally from *I v. Finland* (no. 20511/03, 17 July 2008). In that case, there were flaws in the records system which did not allow the authorities to retroactively clarify how patient records had been used. The fact that the system had revealed only the five most recent consultations, combined with the fact that the health records could have been read by colleagues of the applicant who had not been involved in her treatment, was decisive for the Court's conclusion that Article 8 had been violated (ibid., § 41).

48. In contrast, in the present case, the comprehensive activity logs, coupled with the technical access checks, enabled the NAV's data protection unit to investigate – both before and during the domestic proceedings – the historical processing of the applicant's data by the individuals of whom she was suspicious. The investigations confirmed that those whose names appeared in the logs and who had had access to the applicant's case file had been involved in the processing of her benefits. Not everyone who forwarded tasks had access to health information, as only those with the required access rights could access health documents. The Court of Appeal concluded that the NAV, as an employer, had not had access to the applicant's medical files, and that none of her four colleagues in the NAV's Nordstrand office who had had the relevant access rights had been "snooping around" in her case file (see paragraph 19 above).

49. The Court notes that the applicant's claim for damages was fully examined by the national courts, and that she did not specify how much she

was claiming. The Court of Appeal found that she had not suffered any damage as a result of an infringement of the GDPR. The court also considered whether it was reasonable to award the applicant compensation under section 30 of the Personal Data Act, ultimately dismissing her claim in that regard (see paragraph 19 above).

50. The Court considers that the applicant's complaints were extensively investigated and examined at national level, and that the reasoning and conclusions drawn by the domestic courts were both relevant and sufficient. The applicant's complaints led to changes being made to the NAV's data protection procedures in 2020, which means that the State was fully compliant with its obligations under the GDPR by then. A fair balance was thus struck between the competing interests.

51. The foregoing considerations are sufficient to enable the Court to conclude that, at the relevant time, the State did not fail in its positive obligation under Article 8 § 1 of the Convention to ensure respect for the applicant's private life.

52. Accordingly, the applicant's complaint under Article 8 of the Convention is manifestly ill-founded within the meaning of Article 35 § 3 (a) and must be rejected pursuant to Article 35 § 4.

B. Complaint under Article 13 of the Convention

53. The applicant considers that she did not have at her disposal any effective domestic remedy to complain about the alleged breach of her rights under Article 8. She invokes Article 13, which reads as follows:

> "Everyone whose rights and freedoms as set forth in [the] Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

54. According to the Court's case-law, Article 13 cannot reasonably be interpreted so as to require a remedy in domestic law in respect of any supposed grievance under the Convention that an individual may have, no matter how unmeritorious his complaint may be: the grievance must be an arguable one in terms of the Convention (see *Boyle and Rice v. the United Kingdom*, 24 April 1988, § 52, Series A no. 131). In the present case, the Court has concluded that the applicant's substantive claim was manifestly ill-founded. The rejection of a complaint as "manifestly ill-founded" amounts to a decision that "there is not even a prima facie case against the respondent State" (see *Airey v. Ireland*, 9 October 1979, § 18, Series A no. 32). The Court is therefore of the opinion that in the circumstances of the present case, the applicant did not have any arguable grievance in terms of the Convention and that Article 13 does not apply (see, *mutatis mutandis*, *Walter v. Italy* (dec.), no. 18059/06, 11 July 2006).

55. It follows that this complaint is incompatible *ratione materiae* with the provisions of the Convention within the meaning of Article 35 § 3 and must be rejected in accordance with Article 35 § 4.

For these reasons, the Court, unanimously,

Declares the application inadmissible.

Done in English and notified in writing on 2 April 2026.

Andrea Tamietti Registrar	Jovan Ilievski President