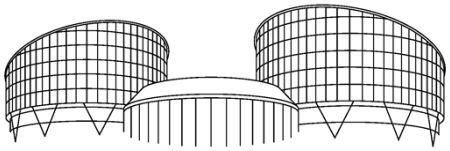

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

FIFTH SECTION

CASE OF SURIKOV v. UKRAINE

(Application no. 42788/06)

JUDGMENT

STRASBOURG

26 January 2017

FINAL

26/04/2017

This judgment has become final under Article 44 § 2 of the Convention. It may be subject to editorial revision.

In the case of Surikov v. Ukraine,

The European Court of Human Rights (Fifth Section), sitting as a Chamber composed of:

Angelika Nußberger, *President,*
Ganna Yudkivska,
André Potocki,
Faris Vehabović,
Síofra O'Leary,
Carlo Ranzoni,
Mārtiņš Mits, *judges,*
and Milan Blaško, *Deputy Section Registrar,*

Having deliberated in private on 13 December 2016,

Delivers the following judgment, which was adopted on that date:

PROCEDURE

1. The case originated in an application (no. 42788/06) against Ukraine lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by a Ukrainian national, Mr Mikhail Mikhaylovich Surikov ("the applicant"), on 29 September 2006.

2. The applicant, who had been granted legal aid, was represented by Ms V.A. Sakhanskaya, a lawyer practising in Simferopol. The Ukrainian Government ("the Government") were represented, most recently, by their acting Agent, Ms O. Davydchuk.

3. The applicant alleged, in particular, that his employer had arbitrarily collected, retained, used and disseminated his mental-health data and that the domestic courts had failed to respond to his relevant arguments.

4. On 17 October 2011 the application was communicated to the Government.

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

5. The applicant was born in 1962 and lives in Simferopol.

A. History of the applicant's employment with the publisher Tavrida

6. In 1990 the applicant graduated from the Ukrainian Printing and Publishing Institute with a diploma in technological engineering.

7. On 23 August 1990 he was employed as a worker by the Tavrida State Publishing House (hereafter "Tavrida").

8. In June 1997 the applicant asked N., the director of Tavrida, to place him on the reserve list for promotion to an engineering position corresponding to his qualifications.

9. Having received no follow-up, in 2000 the applicant applied for the second time.

10. On 6 March 2000 this application was refused.

11. On an unspecified date in 2000 the applicant appealed to the Central District Court of Simferopol (hereinafter "the Central District Court") seeking, in particular, to oblige his employer to consider him for an engineering position.

12. During the proceedings, the defendant company submitted that its refusal was connected to the state of the applicant's mental health. In particular, as was apparent from the information retained on the applicant's personnel file, in 1981 he had been declared unfit for military service in peacetime in accordance with Article 5b of the then applicable 1973 Diseases and Handicaps Schedule issued by the Ministry of Defence of the Union of Soviet Socialist Republics ("the USSR"). In the summer of 1997 the human resources department had obtained from the military enlistment office a certificate stating that the applicant had indeed been dispensed under Article 5b, which read as follows: "psychosis and psychotic disorders connected to organic cerebral lesions with residual moderately manifested deviations in the mental sphere". The defendant company further noted that as the applicant had not provided any subsequent information concerning his state of health, his appointment to an engineering position – which implied managerial responsibilities and supervision of other employees – was considered unwarranted. A copy of the certificate issued by the military enlistment office was provided to the court for examination during the public hearings.

13. B., the applicant's supervisor questioned by the court during the trial, submitted that the applicant had been a diligent employee. However, in his view he lacked the necessary personal skills to occupy a position with managerial responsibilities. In particular, occasionally the applicant had been involved in conflicts with his colleagues. All of them, when questioned by B., had suggested that they did not want to have the applicant as their supervisor. In view of the above and with regard being had to the reasons for the applicant's dispensation from military service, in B.'s view the management had been correct in refusing the applicant's application for promotion.

14. On 17 August 2000 the court rejected the applicant's claim, having found that promotion of employees was within the employer's discretion and there was no legal basis for obliging the defendant company to arrange the applicant's promotion by way of court proceedings in a situation such as that of the applicant.

15. On 24 September 2000 this judgment was upheld by the Supreme Court of the Autonomous Republic of Crimea ("the ARC") and became final.

16. In 2002 Tavrida referred the applicant for a medical examination "with a view to determining [his] fitness for employment" as an engineer.

17. On 5 September 2002 the applicant obtained a certificate signed by six medical specialists, including a psychiatrist and a neurologist from the local polyclinic attesting to his fitness for employment as an engineer.

18. In August 2003 the applicant was appointed as a foreman and in April 2006 as an engineer-technologist.

B. Data protection proceedings against Tavrida

19. In October 2000 the applicant instituted civil proceedings against Tavrida seeking damages and apologies from its management for his purported defamation resulting from the dissemination of information concerning the medical grounds for his dispensation from military service. He alleged, in particular, that the defendant company had had no right to enquire of the enlistment office in 1997 about the grounds for his dispensation, to use this information in deciding on his promotion and to disseminate it to his direct supervisor and other colleagues, as well as to communicate it to the court in the framework of the civil dispute.

20. In January 2001 the applicant modified his claims, seeking to oblige the defendant company, in particular, to promote him to an engineering position and to pay him non-pecuniary damages for the purportedly unlawful processing of his health data, libel, and discrimination on the basis of health.

21. On 23 January 2001 the Central District Court rejected the applicant's claim as lacking legal basis. In particular, it noted that labour law did not prohibit employers from enquiring of military enlistment offices about their employees' military service records.

22. On 28 March 2001 the Supreme Court of the ARC quashed this judgment and remitted the case for a fresh consideration. It noted that pursuant to section 23 of the Information Act of 1992, health data constituted personal data and could only be collected with the applicant's consent, unless otherwise envisaged by law. The trial court should have established whether it had been lawful to collect and use the applicant's psychiatric health data in the manner and in the context in which it had been used; what the purpose of its processing had been and whether it had been justified, regard being had, in particular, to the fact that the data pertained to 1981. The court also noted that section 46 of the Information Act expressly restricted dissemination of confidential medical information. The trial court should have explored whether the enlistment office's certificate contained

confidential medical information and whether the fact that it had become known to other employees had caused damage to the applicant.

23. In May 2002 the applicant further amended his claim, alleging that the defendant company had processed his health data in breach of: Article 32 of the Constitution of Ukraine; sections 23 and 46 of the Information Act; section 40 of the Legislative Guidelines concerning Protection of Health in Ukraine ("the Health Protection Guidelines"); and sections 3 and 6 of the Psychiatric Assistance Act.

24. On 17 May 2002 the Central District Court rejected the applicant's claim, having requalified it in law as falling within the ambit of Article 7 of the Civil Code of Ukraine of 1963 as in force at the material time and found that the defendant company could not be held liable under that provision for having disseminated defamatory statements. It also noted that the information obtained by the defendant company from the enlistment office, could not qualify as "confidential medical information", as it contained a reference to the standardised grounds for dispensation from military service rather than a personalised medical diagnosis.

25. On 19 February 2003 the Court of Appeal of the ARC (formerly the Supreme Court of the ARC; hereinafter "the Court of Appeal") quashed this judgment and remitted the case for a fresh consideration. It noted, in particular, that the Central District Court had arbitrarily requalified the applicant's claims as falling within the ambit of Article 7 of the Civil Code rather than addressing his arguments concerning the breach of the legal provisions to which he had referred. It further instructed the District Court to take into account the ruling of the Constitutional Court of Ukraine of 30 October 1997 in the case of *Ustymenko* in interpreting applicable legislation.

26. On 23 July 2003 the Central District Court took a fresh decision rejecting the applicant's claims, referring, again, to Article 7 of the Civil Code and having found that there was nothing unlawful either in Tavrida's or its director's personal conduct with respect to the processing of the disputed information. Without referring to any legal provisions, the court noted that the director had been authorised to know the reasons for the applicant's dispensation from military service, as this information had been a part of the personnel record compiled and kept by employers in the ordinary course of business. Discussion of the relevant information with some other company employees had been carried out in good faith: it had only happened in the context of taking a decision on whether the applicant could be appointed to a position with increased responsibilities, including staff management. In doing so, the director had acted within the limits of managerial discretion.

27. The applicant appealed against this decision. He submitted, in particular, that the information concerning the standardised grounds for his dismissal in 1981 had not been specific enough to serve as a basis for determination of whether or not he could be employed as an engineer in

1997; and that in any case it had been outdated. Should his employer have had any doubts concerning his psychiatric health, it could have asked the applicant to provide a current medical certificate of fitness for work. He further noted that the court had not addressed his arguments under Article 32 of the Constitution of Ukraine, the Information Act and other legal provisions to which he had referred. In addition, the applicant noted that the Central District Court had not cited any references to any legal provisions entitling employers to enquire without their employees' consent about the reasons for their dispensation from military service, and to have them recorded in their personnel files. In the applicant's view, this information was not pertinent to his ability to perform engineering duties. The court had also not assessed whether it had been justifiable to communicate the information concerning the applicant's dispensation to third parties.

28. On 1 December 2003 the Court of Appeal rejected the applicant's appeal, upholding the final conclusions reached by the Central District Court, but having amended the reasoning. In particular, it found that Tavrida had been an improper defendant in the applicant's case, as the applicant's complaint in substance had concerned the conduct of N. (its director); K. (the human resources officer); and B. (the applicant's supervisor) acting in their capacity as individuals. The Court of Appeal did not cite any legal provisions in substantiation of its conclusions.

29. The applicant appealed on points of law arguing that N., K. and B. had been acting in their official capacities when processing his health data, thus the defendant company had been vicariously liable for their actions. He further noted that in any event the court had had the authority to summon the proper defendants in the case, rather than dismissing it, and that both the trial and the appeal courts had never considered his main arguments on the merits.

30. On 29 May 2006 the Supreme Court of Ukraine refused the applicant's application for leave to appeal on points of law.

C. Data protection proceedings against Tavrida's officers

31. In July 2006 the applicant instituted civil proceedings challenging, in particular, the lawfulness of the actions of N., K. and B. with respect to the processing of his health data.

32. On 30 November 2006 the Kyivskiy District Court of Simferopol rejected the applicant's claim as unsubstantiated. The court acknowledged that the disputed data qualified as "confidential information" falling within the ambit of section 23 of the Information Act. At the same time, it noted that the scope of individual involvement of each of the defendants in collecting and processing this information was not entirely clear. In any event, this processing had been lawful, as according to applicable law, the

human resources departments were obliged to keep the military duty records of their staff on file and to synchronise them with the military enlistment offices. The communication of the relevant information by the human resources officer to the company director in connection with deciding on the applicant's promotion had also been justified, because managers had been entitled to be apprised of their employees' health, such information being necessary for ensuring a safe working environment. The defendants had obtained access to the disputed information in accordance with the law and processed it for the sole purpose of deciding on the applicant's promotion; this processing had been carried out in good faith and so had not been unlawful.

33. The applicant appealed against this decision, alleging, *inter alia*, that using (in 1997 and 2000) the information concerning the reasons for his dispensation from military service in 1981 with a view to deciding on his promotion had been excessive; that the relevant information had been outdated, incomplete and impertinent; and that should his employer have wanted to check his health status, it should have referred him to a specialised medical commission.

34. On 24 January 2007 the Court of Appeal rejected the applicant's appeal.

35. On 23 May 2007 the Supreme Court rejected a further application by the applicant for leave to appeal on points of law.

II. RELEVANT DOMESTIC LAW AND INTERNATIONAL MATERIALS

A. Relevant domestic law and practice

1. Relevant legal provisions and case-law concerning protection of personal data and confidentiality of medical information

(a) Constitution of Ukraine of 1996

36. Article 32 of the Constitution of Ukraine, which is the relevant provision, reads as follows:

Article 32

"No one shall be subject to interference in his or her personal and family life, except in cases envisaged by the Constitution of Ukraine.

The collection, storage, use and dissemination of confidential information about a person without his or her consent shall not be permitted, except in cases determined by law, and only in the interests of national security, economic welfare and human rights.

...

Everyone is guaranteed judicial protection of the right to rectify incorrect information about himself or herself and members of his or her family, and of the right to demand that any type of information be expunged, and also the right to compensation for material and moral damages inflicted by the collection, storage, use and dissemination of such incorrect information."

(b) Civil Code of Ukraine of 1963 (repealed with the effect of 1 January 2004)

37. The text of Article 7 of the Civil Code of Ukraine of 1963, in force at the material time, in so far as relevant, can be found in the Court's judgment in the case of *Ukrainian Media Group v. Ukraine* (no. 72713/01, § 23, 29 March 2005).

(c) Law of Ukraine "On Information" (Information Act) no. 2657-XII of 2 October 1992

38. The relevant provisions of the Information Act, as worded in the material time, read as follows:

Section 23. Information concerning a person

"Information concerning a person is a complex of documented or publicly acclaimed pieces of information about a person.

The main data concerning a person (personal data) are nationality, education, family status, religious convictions, state of health, as well as address, date and place of birth.

...

The collection of information concerning a person without [the subject's] prior permission is prohibited except for in cases envisaged by law ..."

Section 31. Access of citizens to information concerning them

"Citizens shall be entitled to:

- know at the moment of collection of information, what data pertaining to their person and for what purpose is collected; how, by whom, and for what purpose it is used;

- to access information concerning themselves, file objections concerning its accuracy, completeness, pertinence, etc.;

State bodies and organisations, ... information systems of which contain information about citizens, shall be obliged to ... take measures with a view to prevention of unauthorised access to it. ...

Prohibited shall be access of third parties to information concerning another person, collected in accordance with applicable legislation by the State bodies, organisations and officials.

Storage of information concerning citizens shall not exceed the period necessary for a purpose established by law.

...

Necessary amount of data concerning citizens, which may be obtained by lawful means, must be as limited as possible and may be used only for a legally established purpose.

Refusal of access to such information or its concealment, unlawful collection, use, storage or disclosure may be challenged in a court of law."

Section 46 Prohibition of abuse of the right to information

"...

There should be no dissemination of confidential medical information ... except for in cases envisaged by law."

(d) Law of Ukraine "On Legislative Guidelines concerning Protection of Health in Ukraine ("the Health Protection Guidelines") no. 2801-XII of 19 November 1992

39. Section 40 of the aforementioned Act reads as follows:

Section 40. Confidential Medical Information

"Medical staff and other persons who, in connection with the execution of their professional or official duties, have become apprised of a disease, medical certification, examination, and their results; [as well as] of aspects of the intimate and family spheres of life of a citizen, shall not have the right to disseminate this information, other than in cases envisaged by law ..."

(e) Law of Ukraine "On Psychiatric Assistance" ("Psychiatric Assistance Act") no. 1489-III of 22 February 2000

40. The relevant provisions of the aforementioned Act read as follows:

Section 3. Presumption of mental health

"Each individual shall be considered as having no mental disorders until the presence of such a disorder is established on the grounds of and according to the procedure established by this Act and other laws of Ukraine."

Section 6. Confidentiality of data concerning an individual's state of mental health and provision of psychiatric assistance

"Members of medical staff ... and persons, who, in connection to their studies or performance of professional, official, public or other duties have become apprised that an individual suffers from a mental disorder, ... as well as of other data concerning the state of an individual's mental health [or] his or her private life, may not disclose this data, except in accordance with ... this section.

...

The documents that comprise information concerning the state of a person's mental health and provision to him or her of psychiatric aid must be stored in compliance with requirements which secure the confidentiality of this information. The provision of the originals of these documents and the making of copies can be carried out only in cases established by law. ..."

(f) Ruling of the Constitutional Court of Ukraine of 30 October 1997 in the case concerning official interpretation of sections 3, 23, 31, 47, 48 of the Information Act and section 12 of the Law of Ukraine "On the Prosecutor's Office" (case of *K.G. Ustymenko*, no. 18/203-97)

41. The relevant parts of the aforementioned Ruling read as follows:

"...

2. ... analysis of the application of the law [and analysis] of the evidence presented in the current constitutional complaint gives grounds for stating that the applicable law on information processing contains poorly defined, contradictory provisions and loopholes which negatively affect the protection of the constitutional rights and freedoms of a human and a citizen.

..., part two of Article 32 of the Constitution of Ukraine bans the collection, storage, use and dissemination of confidential information concerning a person without his or her consent, except in cases determined by law, and only in the interests of national security, economic welfare and human rights. However, national legislation is not comprehensive in determining the [relevant procedures], in particular, as concerns the mental state of an individual ...

The legislation of Ukraine has not been harmonised with the European personal data protection standards in connection with the accession of Ukraine to the Council of Europe ...

Based on the above, ... the Constitutional Court holds:

1. Part four of section 23 of the Information Act shall be understood as prohibiting not only collection, but also storage, use and dissemination of confidential information concerning a person without his/her prior consent, except in cases, established by law, and only in the interests of national security, economic welfare and human rights and freedoms. Confidential information shall include, in particular, personal details (education, family status, religious convictions, state of health, date and place of birth, financial standing and other personal data) ..."

2. Relevant domestic law concerning employers' duty to create a safe working environment for their employees and to maintain military duty register

(a) Code of the Labour Laws of Ukraine (Labour Code) of 1971

42. The relevant provisions of the Labour Code as worded at the material time read as follows:

Article 2. Basic labour rights of the employees

"...

Employees shall be entitled to ... a healthy and safe working environment ..."

Article 153. Creation of safe and non-harmful working environment

"...

Creation of a safe and non-harmful working environment shall be vested in the owner or the authority empowered by him or her ..."

(b) Law of Ukraine "On Military Duty and Mandatory Military Service"(the Military Service Act) no. 2232-XII of 25 March 1992

43. Pursuant to section 35 of the aforementioned Act, as adopted in 1992, public and private entities employing individuals liable to be drafted for military service or to be called up were under an obligation to keep records listing the personal details of such individuals. The executives of such entities bore personal responsibility for the proper organisation of such record-keeping. Following revision of this Act on 18 June 1999, the same obligation was envisaged in the new section 34.

(c) Instruction on maintenance of a military register of persons liable for military service and call-up in the enterprises, institutions, organisations and educational facilities approved by Order of the Minister of Defence of Ukraine no. 165 of 27 June 1995 (Instruction no. 165)

44. Pursuant to section 10 of the above Instruction (repealed by Order of the Minister of Defence of Ukraine no. 660 of 15 December 2010), employers were obliged to maintain the register of their employees liable for military service and call-up (military duty register) for the purpose of "ensuring ... compliance by the citizens of Ukraine with their military duty ...".

45. In accordance with sections 13 and 19, this register was made up of a structured filing system comprised of the standardised personnel record cards of employees categorised with respect to their military duty eligibility. The standardised text of such cards was provided in the annex.

46. In accordance with section 14, basic entries onto the personnel cards were to be copied from the individual military identification and registration documents, such as the "military identification card" (*військовий квиток*) issued by the authorities to citizens liable for military duty.

47. In accordance with section 15 employers were to enter on the personnel cards of their employees, among other data, the information concerning their fitness for military service. If an employee had been declared unfit for military service in peacetime, the relevant entry had to include a reference to the Article of the applicable Diseases and Handicaps Schedule issued by the Minister of Defence, on the basis of which this employee had been dispensed from military service.

48. In accordance with section 19, the military duty register was to be kept in accordance with the procedures established for classified (secret) documents.

49. Pursuant to section 20, both public and private employers were obliged to demand military service eligibility documents from their prospective employees, and could not employ a person whose relevant status or documents had not been regularised.

50. Various provisions of the Instruction also stipulated a duty of employers to synchronise regularly their records with those of the military enlistment offices and a duty of citizens liable for military service to inform

the competent authorities of any changes in their status, including health status.

(d) Order of the Ministry of Defence of the USSR no. 185 of 3 September 1973

51. In accordance with Article 5b of the Schedule of health disorders and physical handicaps ("the Diseases and Handicaps Schedule") annexed to the above order enacted in 1973, individuals certified by specialised medical commissions as suffering from "*psychosis and psychotic disorders connected to organic cerebral lesions with residual moderately manifested disorders in the mental sphere*" were declared unfit for military service in peacetime and fit for noncombatant service in wartime.

52. On 9 September 1987 the aforementioned Order was replaced by Order of the Ministry of Defence of the USSR no. 260, which included a new Diseases and Handicaps Schedule. Following Ukraine achieving independence, on various subsequent dates new Schedules were issued by the orders of the Minister of Defence of Ukraine.

B. Relevant Council of Europe materials

53. Convention ETS No. 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data ("the Data Protection Convention") was adopted on 28 January 1981 and subsequently ratified by all Council of Europe member States.

54. This Convention was signed by Ukraine on 29 August 2005 and ratified on 30 September 2010.

55. Its relevant provisions read as follows:

Article 3. Scope

"1. The Parties undertake to apply this Convention to automated personal data files and automatic processing of personal data in the public and private sectors.

2. Any State may ... give notice by a declaration addressed to the Secretary General of the Council of Europe:

...

c. that it will also apply this Convention to personal data files which are not processed automatically.

..."

Article 5. Quality of data

"Personal data undergoing automatic processing shall be:

a. obtained and processed fairly and lawfully;

b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

c. adequate, relevant and not excessive in relation to the purposes for which they are stored;

d. accurate and, where necessary, kept up to date; ...”

Article 6. Special categories of data

“Personal data ... concerning health ... may not be processed automatically unless domestic law provides appropriate safeguards ...”

Article 7. Data security

“Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.”

Article 10. Sanctions and remedies

“Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.”

C. Other relevant international materials

1. The European Union law

56. *Charter of Fundamental Rights of the European Union* (2000/C 364/01) proclaimed on 7 December 2000, which came into force on 1 December 2009 includes right to the protection of personal data among the fundamental rights. Article 8 of the Charter provides, in particular, as follows:

Article 8. Protection of personal data

“1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. ...”

57. *Directive 95/46/EC of the European Parliament and of the Council of the European Union on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (“the EU Data Protection Directive”) of 24 October 1995 provides that the object of national laws in this area is notably to protect the right to privacy as recognised both in Article 8 of the Convention and the general principles of EU law. The Directive defines personal data as “any information relating to an identified or identifiable natural person” (Article 2(a)) and asks for the member States to prohibit processing of personal data concerning “health” among other things (Article 8(1)).

58. As of 25 May 2018 the Directive will be replaced by *Regulation (EU) 2016/679 of the European Parliament and of the Council on the*

protection of natural persons with regard to the processing of personal data and on the free movement of such data. This regulation was adopted on 27 April 2016 with a view to ensuring further harmonisation of the data protection legal framework within the European Union member States. According to Article 9, paragraph 1 of the Regulation, processing of data concerning health shall be prohibited, unless such processing falls within one of the exceptions listed in paragraph 2. Notably, processing of health data for the assessment of the working capacity of an employee shall be allowed when those data would be processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies (see Article 9 paragraph 2 point (h), and paragraph 3).

2. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("the OECD Privacy Guidelines")

59. On 23 September 1980 the Organisation for Economic Co-operation and Development ("the OECD") adopted the Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (C(80)58/FINAL) reflecting the consensus among its member States that basic principles of fair personal information processing in the public and private sectors should be safeguarded in the national legislative frameworks. In 2013 the revised Guidelines were adopted.

60. According to part 1, section 2 of the original Guidelines, they were intended to apply to personal data in both the public and private sectors, "which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties". The original Guidelines included the following basic principles, among others:

Collection Limitation Principle

"7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."

Data Quality Principle

"8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date."

Purpose Specification Principle

"9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of

those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose."

Use Limitation Principle

"10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law."

Security Safeguards Principle

"11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data."

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

61. The applicant complained that his employer had arbitrarily collected, retained, and used sensitive, obsolete and irrelevant data concerning his mental health in considering his application for promotion, and had unlawfully and unfairly disclosed this data to the applicant's colleagues and to a civil court during a public hearing. The applicant relied on Article 8 of the Convention, which reads as follows:

"1. Everyone has the right to respect for his private ... life ... .

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."

A. Admissibility

62. The Government did not comment on the admissibility of the present complaint.

63. The Court notes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention. It further notes that it is not inadmissible on any other grounds. It must therefore be declared admissible.

B. Merits

1. Submissions by the parties

(a) The applicant

64. In his application and subsequent observations, the applicant noted that when taking up employment with Tavrida he had provided its human resources department with a copy of his military identification card for entering his data onto the military duty register maintained by the company, in accordance with the applicable law. This card had contained a reference to Article 5b of the Diseases and Handicaps Schedule issued in 1973, on the basis of which in 1981 the applicant had been declared unfit for military service in peacetime. No text from this Article had appeared on the above document. Tavrida had acted unlawfully in 1997 in obtaining the wording of this Article, which contained sensitive medical data, from the military enlistment office without the applicant's knowledge or consent. It had also acted unlawfully in including this information in the applicant's personnel file in spite of its retention patently having been excessive for the purposes for which it had been kept. Next, Tavrida had acted unlawfully in using this information for a new purpose, that is to say for assessing and turning down the applicant's applications for promotion in 1997 and 2000, in spite of the fact that this information had been very old and of inadequate detail for determining the applicant's fitness for the position he sought. Above all, Article 5b of the Diseases and Handicaps Schedule was insufficiently specific. It applied equally to persons suffering from very serious psychotic disorders and to those suffering from mild temporary conditions. In fact, the applicant had never been in a psychotic state. Making any conclusions concerning his mental health on the basis of the information contained in this Article had created a false appearance that he might have suffered from a very serious disorder. Should the applicant's employer have been concerned about his mental health in terms of his promotion, it could have solicited more recent and specific information, in particular by referring the applicant to a medical commission for the assessment of his fitness for promotion. Having obtained such a referral in 2002, the applicant had duly passed the necessary assessment and had eventually been placed on the reserve list and then promoted to an engineering position.

65. Lastly, the applicant complained that in the context of discussing his promotion applications, the information concerning the medical grounds for his dispensation from military service had been communicated, in breach of domestic medical confidentiality rules, to his co-workers, including B., his direct supervisor, and subsequently to the civil court in the course of a public hearing in context of the proceedings in which he had complained about the rejection of his promotion applications. Such disclosure had caused him mental suffering and had negatively affected his relationships with his colleagues.

(b) The Government

66. The Government contended that the disputed conduct of the applicant's employer had not constituted an interference with his rights guaranteed by Article 8.

67. First of all, the information concerning the grounds for the applicant's dispensation from military service had not been confidential. In particular, the Diseases and Handicaps Schedules had been published and publicly consultable. Pursuant to the applicable laws, in particular, section 34 of the Military Service Act and Military Register Maintenance Instruction no. 165, the applicant's employer had been obliged to copy the information concerning the grounds for his dispensation contained on his military identification card onto his personnel record card for storage in the standardised filing system. The fact that the information entered initially had not used the exact wording of Article 5b was immaterial in this context, as the Diseases and Handicaps Schedules had been accessible by the public. By contacting the military enlistment office in 1997, Tavrida had simply confirmed the information which had already been provided by the applicant himself, rather than actually obtaining additional information. In the Government's view, this situation was factually comparable to that examined by the Court in the case of *N.F. v. Italy* (no. 37119/97, ECHR 2001-IX). In particular, in that case the Court had found that the applicant's complaint about disclosure by the press of his membership of a registered Freemason's lodge had not affected his rights under Article 8, as that lodge's members' register had in any event been publicly consultable.

68. The Government also noted that the disputed information had only become available to the human resources department of the applicant's employer and to its director, who had been entitled to it under the applicable law. As regards any further dissemination, in their view, regard being had to the findings of the domestic courts, the relevant facts had not been proven.

69. In addition to that, the Government also relied on the provisions of Articles 2 and 153 of the Labour Code, which outlined employees' right to a safe and healthy working environment and their employers' corresponding duty to ensure it.

2. The Court's assessment

(a) General principles

70. On numerous occasions the Court has held that systematic storage and other use of information relating to an individual's private life by public authorities entails important implications for the interests protected by Article 8 of the Convention and thus amounts to interference with the relevant rights (see, in particular, *Rotaru v. Romania* [GC], no. 28341/95, § 46, ECHR 2000-V; and *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 67, ECHR 2008). This is all the more true

where the information concerns a person's distant past (see *Rotaru*, cited above, § 43, and *M.M. v. the United Kingdom*, no. 24029/07, § 187, 13 November 2012) or when the processing affects highly intimate and sensitive categories of information, notably the information relating to physical or mental health of an identifiable individual (see, in particular, *Z. v. Finland*, 25 February 1997, § 95, Reports of Judgments and Decisions 1997-I; *I. v. Finland*, no. 20511/03, § 40, 17 July 2008; *P. and S. v. Poland*, no. 57375/08, § 128, 30 October 2012; *L.H. v. Latvia*, no. 52019/07, § 56, 29 April 2014; and *Y.Y. v. Russia,* no. 40378/06, § 38, 23 February 2016).

71. The Court next reiterates that an interference breaches Article 8 unless it is "in accordance with the law", pursues one or more of the legitimate aims referred to in paragraph 2 and is, in addition, "necessary in a democratic society" to achieve those aims (see, among other authorities, *P. and S. v. Poland*, cited above, § 94, and *M.N. and Others v. San Marino*, no. 28005/12, § 71, 7 July 2015). The Court reiterates from its well established case-law that the wording "in accordance with the law" requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, that is to say to be accessible, foreseeable and accompanied by necessary procedural safeguards affording adequate legal protection against arbitrary application of the relevant legal provisions (see, among other authorities, *S. and Marper*, cited above, § 95, and *M.N. and Others,* cited above, § 72).

72. The function of clarification and interpretation of the provisions of domestic law belongs primarily to domestic judicial authorities. In order to protect a person against arbitrariness, it is not sufficient to provide a formal possibility of bringing adversarial proceedings to contest the application of a legal provision to his or her case. Domestic courts must undertake a meaningful review of the authorities' actions affecting rights under the Convention in order to comply with the lawfulness requirement (see *Y.Y.,* cited above, § 50).

73. In addition to being lawful, the interference must also pursue a legitimate aim and be "necessary in a democratic society". In determining whether the impugned measures were "necessary in a democratic society", the Court will consider whether, in the light of the case as a whole, the reasons adduced to justify them were relevant and sufficient and the measures were proportionate to the legitimate aims pursued (see, for example, *Peck v. the United Kingdom*, no. 44647/98, § 76, ECHR 2003-I). In this latter respect the Court has noted that, regard being had to the fundamental importance of data protection for effective exercise of one's right to respect for private life, the margin of appreciation afforded to the member States in designing their respective legislative and administrative frameworks in this sphere is rather limited (see, in particular, *Peck,* cited above, §§ 77-78; and *S. and Marper*, cited above, §§ 102-103). In this connection, the question of "necessity of interference" may overlap with the question concerning quality of the requisite procedural safeguards afforded

in the domestic law of the respondent State (*S. and Marper*, cited above, § 99, and *Avilkina and Others,* cited above, § 37).

74. To date, a certain level of consensus on the international level and, in particular, between the Council of Europe member States has been achieved as regards the fundamental data protection principles and the corresponding basic procedural safeguards to be included in the national legislative frameworks in order to justify the necessity of any possible interference. These principles were formulated in a number of treaties and other legal instruments, including the *Council of Europe Data Protection Convention no. 108* and other documents (see paragraphs 53-60 above). The Court has previously referred to the relevant international instruments, most notably the *Data Protection Convention*, in assessing data processing and protection practices in individual cases brought under Article 8 of the Convention. In particular, drawing from that Convention, the Court has stated that the domestic law of the member States should notably ensure that personal data in issue are relevant and not excessive in relation to the purposes for which they are being collected or stored; that they are preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored and that the retained data are efficiently protected from misuse and abuse (see, among other authorities, *Gardel v. France*, no. 16428/05, § 62, ECHR 2009). In line with internationally recognised data protection principles, the Court has also stated that it was essential for the applicable law to provide clear, detailed rules governing the scope and application of the relevant measures; as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for their destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness at each stage of its processing (see, in particular, *S. and Marper*, cited above, § 99 and the references therein, and *M.M. v. the United Kingdom*, cited above, § 195). There are various crucial stages at which data protection issues under Article 8 of the Convention may arise, including during collection, storage, use and communication of data. At each stage, appropriate and adequate safeguards which reflect the principles elaborated in applicable data protection instruments must be put in place in order to justify the necessity of interference under Article 8 (see *M.M. v. the United Kingdom*, cited above, ibid).

(b) Application of these principles in the present case

(i) Applicability of Article 8

75. The Court notes that the information at stake in the present case concerned an indication that in 1981 the applicant had been certified as suffering from a mental health related condition. The Court concludes that such information by its very nature constitutes highly sensitive personal

data regardless of whether it was indicative of a particular medical diagnosis. Collection, storage, disclosure and other types of processing of such information fall therefore within the ambit of Article 8.

(ii) Whether there was an interference

76. The Court next notes that at the time of the events giving rise to the present application Tavrida was a Ukrainian State-owned company, as evidenced in the case-file material. It further notes that by virtue of applicable law that company was obliged to maintain the military duty register of its employees and it was within the framework of fulfilling this duty that the data concerning the grounds for the applicant's dispensation from military service was retained by it. In light of the above, the Court considers that the applicant's complaint falls to be assessed as interference by a public authority with the applicant's exercise of his right to private life (see, in particular, *Copland v. the United Kingdom*, no. 62617/00, § 39, ECHR 2007-I; *Avilkina and others*, cited above, § 31 and, mutatis mutandis, *Vukota-Bojić v. Switzerland*, no. 61838/10, § 47, 18 October 2016).

77. The Court must therefore determine whether this interference was justified under the second paragraph of Article 8.

(iii) Whether the interference was in accordance with the law

78. As regards the lawfulness of the disputed interference, as follows from the Government's submissions, the collection and retention of the disputed data was effected on the basis of section 34 of the Military Service Act and the provisions of Instruction no. 165 (see paragraphs 43-50 above). Use of this data for deciding on the applicant's promotion was, in turn, based on Articles 2 and 153 of the Labour Code (see paragraph 42 above).

79. The Court notes that none of the foregoing provisions was expressly referred to in the relevant domestic courts' judgments. However, in the light of the available materials, and notably, the Government's observations, the Court is prepared to accept that collection, storage, and other use of the applicant's mental health had some basis in domestic law.

80. Insofar as quality, in particular, foreseeability of the applicable law may be concerned, the Court observes that there was apparently considerable disagreement among the various judges involved in the adjudication of the applicant's claims as to the scope and meaning of the applicable legal acts, which resulted in numerous remittals of his case for reconsideration (see paragraphs 21-22, 24-26 and 28-29 above). It appears that this disagreement may have been connected to a structural problem in domestic law. Notably, in its 1997 opinion in the *Ustymenko* case the Constitutional Court generally characterised the national mental-health data protection framework as containing "poorly defined, contradictory provisions and loopholes" and not fully consistent with the international obligations of Ukraine (see paragraph 41 above).

81. At the same time, the Court is not called upon to assess the quality of the applicable data protection framework in the abstract and must rather confine itself as far as possible to examining the particular consequences of application of its provisions in the case before it (see *Zehentner v. Austria*, no. 20082/02, § 60, 16 July 2009). From this perspective, it considers that the question of quality of applicable law in the applicant's case is closely related to the broader issue of whether the interference complained of was necessary in a democratic society (see *S. and Marper*, cited above, § 99, and *Avilkina and Others*, cited above, § 37). The Court will therefore examine the matter in the light of this latter perspective below.

(iv) Whether the interference pursued a legitimate aim

82. The Court notes that the Government have not commented on the aims of the disputed interference. Based on the available materials, the Court considers that the measures complained of could be effected for various legitimate aims, notably protection of national security, public safety, health, and the rights of others, in particular of the applicant's co-workers.

(v) Whether the interference was necessary

83. The Court notes that at the time of the events giving rise to the present application, Ukraine was not a member of the *Data Protection Convention* or any other relevant international instrument. However, at the same time, its national legislation contained a number of safeguards similar to those which were included in these legal acts. Relevant provisions can be found, notably, in the *Information Act of 1992* (see paragraph 38 above) and various acts pertaining to confidentiality of medical information (see paragraphs 39-40 above). However, it appears that these safeguards remained largely inoperative in the applicant's case, both during the processing of his personal data by his employer, and during the examination of his relevant claims by the domestic courts.

(α) As regards the power of collection and retention of the applicant's personal data

84. First of all, in so far as the applicant complained that in the summer of 1997 his employer had collected without requisite justification and retained in his personnel file data which was excessive for the purposes of maintaining the obligatory military duty register of its employees, the Court notes at the outset that the disputed act of collection had taken place before the Convention entered into force in respect of Ukraine (11 September 1997). It is therefore as such outside of the Court's temporal jurisdiction. At the same time, as the applicant's complaint concerns, in essence, not only this initial act, but more broadly the fact that the relevant information was

included in and retained on his file, the Court considers itself competent to address the issue of retention (see *Rotaru*, cited above, § 46).

85. In this connection the Court notes that the information added to the applicant's file in 1997 contained nothing more than the wording of Article 5b of the 1973 Diseases and Handicaps Schedule. A reference to this Article had already been entered in the applicant's file earlier, because this provision indicated the grounds for his dispensation from military service in peacetime. A reference to the grounds for dispensation from military service was a standard and mandatory entry in the military duty register as kept by every employer pursuant to *Instruction no. 165*. As the Court has been informed, the foregoing Schedule was a published document. Accordingly, the text of the aforementioned Schedule being publicly consultable at any point of time, the fact that the applicant's employer obtained it from the military enlistment office in summer 1997 was of secondary importance. It follows that the applicant's employer was in possession of the information concerning the grounds for the applicant's dispensation from military service as a result of the general set-up of the applicable legislative framework, rather than the employer's individual conduct, contrary to what the applicant suggests.

86. The Court next notes that the aforementioned legislative framework essentially resulted in a quasi-automatic entitlement for any employer, whether public or private, to obtain and retain sensitive health-related data concerning any employee dispensed from military service on medical grounds. The Court notes that it is not in a position to substitute itself for the competent domestic authorities in deciding on the modalities of keeping the military duty registers. However, the Court reiterates that core principles of data protection require the retention of data to be proportionate in relation to the purpose of collection and envisage limited periods of storage (see *S. and Marper*, cited above, § 107). In line with this, the Court considers that delegating to every employer a public function involving retention of sensitive health-related data concerning their employees can only be justified under Article 8 if such retention is accompanied by particularly strong procedural guarantees for ensuring, notably, that such data would be kept strictly confidential, would not be used for any other purpose except that for which it was collected, and would be kept up-to-date (see, *mutatis mutandis*, *I. v. Finland*, cited above, § 37, and *mutatis mutandis*, *Gardel*, cited above, §§ 69-70).

87. It appears that *Instruction no. 165* listed some relevant safeguards, in particular a requirement that the military duty register be treated as a classified (secret) document and that the data contained in them be regularly synchronised with that retained by the military enlistment offices (see paragraphs 48 and 50 above). At the same time, notwithstanding these requirements, the applicant's employer retained the information dating back to 1981 and used it for deciding in 1997 and 2000 on the applicant's

requests for promotion, considering it permissible to disclose this information to third parties in this context.

88. The judicial authorities found that such practice was not contrary to the provisions of Article 32 of the Constitution and a number of other legal instruments, to which the applicant referred in his civil proceedings. Without responding directly to the applicant's arguments concerning confidentiality of the disputed data, they essentially concluded that the employer's conduct had been lawful, because the disputed information had once been lawfully obtained and there was no appearance of bad faith in discussing and using it in context of deciding on the question of the applicant's promotion.

89. It follows that applicable law, as interpreted and applied by the domestic courts in the present case, permitted storage of the applicant's health-related data for a very long term and allowed its disclosure and use for purposes unrelated to the original purpose of its collection. The Court considers that such broad entitlement constituted a disproportionate interference with the applicant's right to respect for private life. It cannot be regarded necessary in a democratic society (see also *Avilkina and Others*, cited above, §§ 51-54 and *S. and Marper*, cited above, § 125).

(β) As regards disclosure of the applicant's data to third parties and using it for deciding on his promotion

90. As regards the applicant's further data protection complaints, namely, that his personal data was unfairly disclosed to third parties and used for deciding on his promotion, the Court notes that these complaints are closely interrelated with the complaint concerning the retention of this data without necessary safeguards.

91. The Court recognises that employers may have a legitimate interest in information concerning their employees' mental and physical health, particularly in the context of assigning them certain job functions connected to specific skills, responsibilities or competences. However, it underlines once again that collection and processing of the relevant information must be lawful and such as to strike a fair balance between the employer's interests and the privacy-related concerns of the candidate for the relevant position.

92. In this connection, the Court takes note of the applicant's arguments that by the time his health data originating in 1981 was used for deciding on his promotion (1997 and 2000) it was quite old. In addition to that, as it did not indicate the specific nature of the applicant's medical condition diagnosed at that time, it was also incomplete for the purposes of deciding whether or not he could be entrusted with the requested position. It is also notable that in 2002 the applicant was referred by his employer for a medical examination with a view to determining his fitness for the position he sought to occupy. Having obtained a positive conclusion, he was placed on a reserve list and subsequently promoted to his satisfaction (see

paragraphs 17-18 above). The Court has not been provided with any reasons why this option for determining the applicant's medical fitness could not have been used any earlier.

93. The Court further observes that the applicant explicitly raised the arguments discussed in paragraph 92 above before the domestic courts referring to numerous legal instruments. In the meantime, the final decisions taken by the domestic judicial authorities do not provide any answers to these arguments and refer instead to the management's exclusive discretion in personnel decisions and the applicant's failure to demonstrate that his employer had acted in bad faith. They also noted that he had not ascertained the exact role of the individual officers in disclosing his mental-health data. It is not evident from the text of these judgments that the national courts analysed whether using the disputed data by the applicant's employer in deciding, within its discretion, whether to promote the applicant and rejecting the promotion request on its basis struck a fair balance between the employer's interests and the applicant's privacy-related concerns. The same was also true concerning the applicant's complaint about disclosure of this data to the applicant's co-workers in context of the decision-making procedure and its communication to the court in the course of a public hearing (compare also with *Panteleyenko v. Ukraine*, no. 11901/02, §§ 57-61, 29 June 2006). The crux of the applicant's complaints was therefore left outside the scope of the judicial examination. The judicial authorities have thus not provided relevant and sufficient reasons justifying the necessity of the interference complained of.

94. In the light of the considerations advanced in paragraphs 92 and 93 above, the Court finds that the use of the disputed data for deciding on the applicant's promotion and its unrestricted disclosure to various third parties in this context were not necessary in a democratic society.

(vi) Overall conclusion

95. Regard being had to the Court's findings in paragraphs 89 and 94 above, the Court concludes that there has been a violation of Article 8 in connection with retention and disclosure of the applicant's mental-health data as well as its use for deciding on the applicant's applications for promotion.

II. ALLEGED VIOLATION OF ARTICLE 6 OF THE CONVENTION ON ACCOUNT OF INSUFFICIENT REASONING IN THE DOMESTIC COURTS' JUDGMENTS

96. The applicant also complained that the national judicial authorities had not responded to the principal arguments he had adduced in support of his claims in the data protection proceedings against his employer. He relied

on Article 6 of the Convention, which, in so far as relevant, reads as follows:

> "1. In the determination of his civil rights and obligations ... everyone is entitled to a fair ... hearing ... by [a] ... tribunal ..."

A. Admissibility

97. The Government did not comment on the admissibility of the present complaint.

98. The Court notes that this complaint is closely linked to that examined under Article 8 above. It is not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention and not inadmissible on any other grounds. It must therefore be declared admissible.

B. Merits

99. The applicant did not submit any separate comments on the above complaint after the communication of the case.

100. The Government submitted that there had been no violation of Article 6 in the case at issue. In their view, the present complaint was of a "fourth-instance nature".

101. The Court reiterates that Article 6 obliges the courts to give reasons for their judgments (see, in particular, *Van de Hurk v. the Netherlands*, 19 April 1994, § 61, Series A no. 288). Although this obligation cannot be understood as requiring a detailed answer to every argument, the principle of fairness enshrined in Article 6 would be disturbed if domestic courts ignored a specific, pertinent and important point made by an applicant (see, for example, *Pronina v. Ukraine*, no. 63566/00, § 25, 18 July 2006, and *Siredzhuk v. Ukraine*, no. 16901/03, § 63, 21 January 2016).

102. In paragraphs 88 and 93 above the Court has already noted that the domestic judicial authorities failed to address pertinent and important points raised by the applicant with reference to Article 32 of the Constitution and a number of other specific legal provisions. This failure, which constituted one of the elements on the basis of which the Court has found a violation of Article 8, also constitutes a breach of Article 6.

103. Accordingly, there has been a breach of Article 6 on account of the failure of the domestic courts to state adequate reasons for rejecting the applicant's claims in the data protection proceedings against his employer.

III. ALLEGED VIOLATION OF ARTICLE 6 OF THE CONVENTION ON ACCOUNT OF THE LENGTH OF THE PROCEEDINGS

104. Lastly, the applicant complained, under Article 6 of the Convention, that the data protection proceedings against Tavrida, which lasted from October 2000 until May 2006, had been inordinately lengthy.

105. The Court considers that the period at issue, which lasted less than six years for three instances, was not such as to raise an issue under the impugned provision.

106. This complaint must therefore be declared inadmissible as being manifestly ill-founded, pursuant to Article 35 §§ 3 (a) and 4 of the Convention.

IV. APPLICATION OF ARTICLE 41 OF THE CONVENTION

107. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

108. The applicant claimed 100,000 euros (EUR) in respect of non-pecuniary damage.

109. The Government submitted that this claim was exorbitant and unsubstantiated.

110. The Court considers that the applicant has suffered anguish and distress on account of the facts leading to the finding of a violation in the present case, which cannot be made good by a mere finding of these violations. At the same time, the amount claimed is excessive. Ruling on an equitable basis, the Court awards the applicant EUR 6,000 in respect of non-pecuniary damage.

B. Costs and expenses

111. The applicant did not lodge any claim under this head. Accordingly, the Court does not find any call to give an award.

C. Default interest

112. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT, UNANIMOUSLY,

1. *Declares* the complaint under Article 8, and the complaint under Article 6 concerning failure of the domestic courts to address the crux of the applicant's arguments, admissible and the remainder of the application inadmissible;

2. *Holds* that there has been a violation of Article 8 of the Convention;

3. *Holds* that there has been a violation of Article 6 of the Convention;

4. *Holds*
   (a) that the respondent State is to pay the applicant, within three months from the date on which the judgment becomes final, in accordance with Article 44 § 2 of the Convention, EUR 6,000 (six thousand euros), to be converted into the currency of the respondent State at the rate applicable at the date of settlement, plus any tax that may be chargeable;
   (b) that from the expiry of the above-mentioned three months until settlement, simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

5. *Dismisses* the remainder of the applicant's claim for just satisfaction.

Done in English, and notified in writing on 26 January 2017, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Milan Blaško	Angelika Nußberger
Deputy Registrar	President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the separate opinion of Judges O'Leary and Mits is annexed to this judgment.

A.N.
M.B.

JOINT CONCURRING OPINION OF JUDGES O'LEARY AND MITS

1. We agree with the finding of a violation of Article 8 of the Convention in the circumstances of the present case.

2. The applicant's employer, a state-owned company, retained data relating to his mental health, as they were obliged to do pursuant to domestic law,[1] and arbitrarily used and disclosed this data when considering his application for promotion. Such an interference with the right to privacy breaches Article 8 unless it is "in accordance with the law", pursues one or more legitimate aims and is "necessary in a democratic society" for the achievement of one of those aims.[2]

3. While the majority of our colleagues base their finding of a violation on the absence of any necessity for the interference (see §§ 83–94 of the Chamber judgment), we fail to see, in the circumstances of the instant case, what is gained by proceeding to such an examination of necessity. The Chamber judgment only briefly examines the requirement of lawfulness (see §§ 78-81), albeit clearly highlighting the disagreement between the different national courts as regards the scope and meaning of domestic data protection law. It then goes on to transfer to the examination of necessity issues which essentially concern lawfulness (see, in particular, §§ 81 and 86), adding little, if anything, beyond what a proper examination of lawfulness would and should have contained.

4. In our opinion, the judgment ought to have concentrated on the lawfulness of the interference and, in this regard, on the lack of foreseeability and the quality of the domestic legislation within the meaning of the well-established case-law of the Court. Once this, the crux of the legal problem disclosed by the applicant's complaint had been addressed, there was no need to proceed further.

5. Pursuant to the Court's well-established case-law, the phrase "in accordance with the law" in Article 8 § 2 of the Convention requires not only that the impugned measure needed to have some basis in domestic law, but also refers to the quality of the law in question, which should be adequately accessible and foreseeable as to its effects.[3] A rule is foreseeable

---

[1] See, in particular, section 34 of the Military Service Act described below.

[2] See *M.N. and Others v. San Marino*, no. 28005/12, § 71, 7 July 2015; and *Amann v. Switzerland* [GC], no. 27798/95, § 71, 16 February 2000.

[3] See, for example, in the specific context of Article 8 cases in the field of data protection, *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 95, 4 December 2008 (retention of fingerprints and DNA information in cases where the defendant in criminal proceedings is acquitted or discharged); *M.N. and Others v. San Marino*, cited above, § 72 (information retrieved from banking documents copied and stored without safeguards); *Malone v. the United Kingdom*, 2 August 1984, §§ 66-68, Series A no. 82 (interception of communications and "metering" of telephones by or on behalf of the police); *Rotaru v. Romania* [GC], no. 28341/95, § 55, ECHR 2000-V

if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate his conduct.[4] For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and, accordingly, indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise.[5] The level of precision required of the domestic law – which cannot provide for every eventuality – depends to a considerable degree on the content of the law in question, the field it is designed to cover and the number and status of those to whom it is addressed.[6] Moreover, it is not sufficient to provide a formal possibility of bringing adversarial proceedings to contest the application of a legal provision. Domestic courts must undertake a meaningful review of the authorities' actions affecting rights under the Convention in order to comply with the lawfulness requirement.[7]

6. As indicated in the case file, the impugned data was contained in a certificate relating to the applicant's dispensation from military duty pursuant to Article 5b of the 1973 Diseases and Handicaps Schedule. The human resources department and management of the state-owned company which employed the applicant were able to collect and retain that data on the basis of section 34 of the Military Service Act and Instruction no. 165. Use of this data in the context of the decision on the applicant's promotion was, furthermore, based on the health and safety obligations of an employer under Articles 2 and 153 of the Labour Code. As such, it is clear that the collection and use of the data had a legal basis in domestic law.

7. Pursuant to section 34 of the Military Service Act,[8] public and private entities employing individuals liable to be drafted for military service were obliged to keep records listing the personal details of such individuals. However, this section of the act described the purpose and competence of the relevant entities in a very general fashion.[9] Instruction no. 165 sought to detail the purpose and content of the military duty register as well as

---

(gathering, recording and archiving in secret files of information affecting national security without laying down limits on the exercise of those powers, which remained at the discretion of the authorities.); and *Amann*, cited above, § 56 (interception of a business-related telephone call to the applicant, an investigation of the applicant based on that call and the creation of a card on the applicant for the national security card index.).

[4] See also *Silver and Others v. the United Kingdom*, nos. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, § 88, 25 March 1983.

[5] See *supra* note 2.

[6] See *Delfi AS v. Estonia* [GC], no. 64569/09, §§ 120-121, 16 June 2015, with further references; *S. and Marper v. the United Kingdom*, cited above, § 96, and *Hasan and Chaush v. Bulgaria* [GC], no. 30985/96, § 84, ECHR 2000-XI.

[7] *Y.Y. v. Russia*, no. 40378/06, § 50, 23 February 2016; *Kryvitska and Kryvitskyy v. Ukraine*, no. 30856/03, § 43, 2 December 2010; and *C.G. and Others v. Bulgaria*, no. 1365/07, §§ 42-49, 24 April 2008.

[8] Before the introduction of amendments in 1999, this obligation was prescribed by section 35 of the Military Service Act (see § 43 of the Chamber judgment).

[9] See, in this regard, *L.H. v. Latvia*, no. 52019/07, § 52, 29 April 2014.

employers' duties thereunder. Nevertheless, although Section 19 of the latter provided that the data was to be kept in accordance with the procedure established for classified documents, it was published and publicly accessible. In addition, the provisions of Instruction no. 165 did not provide for a right to be informed of the processing of health-related data or a legal obligation to take decisions concerning the processing of such data by acquiring the data subject's consent.[10] As regards the provisions of the Information Act of 1992, they too were relatively vague, providing, for example, that storage of data "shall not exceed the period necessary for a purpose established by law". At least from the information available in the case file, it is difficult if not impossible to see how the various general and specific provisions touching on data protection interacted with one another, with the Information Act providing numerous exceptions to its protective rules "in cases envisaged by law".

8. It is worth noting that, as regards data processing in Ukraine, the Ukrainian Constitutional Court had held, in a decision of 1997, that the applicable law on information processing contained "poorly defined, contradictory provisions and loopholes which negatively affect the protection of the constitutional rights and freedoms of a human and a citizen" and that "the national legislation is not comprehensive in determining the relevant procedures concerning the mental state of individuals".[11]

9. The Court's case-law states that the nature of health-related data requires it not to be used for any other purpose than that envisaged by the law.[12] As indicated previously, section 34 of the Military Act and Instruction no. 165 oblige employers, both public and private, to keep a standardised reference of the military duty register with respect to each employee's eligibility for military duty. The purpose is thus to ensure employees' compliance with their military duty as stated in section 10 of Instruction no. 165, not to attest to their subsequent fitness for promotion in non-military employment for an undisclosed and/or unlimited period of time. However, as the Chamber judgment recognises in its subsequent examination of the necessity of the interference, the loosely regulated access to and use of the sensitive data in the instant case was the result of the *general set-up of the legislation* and led to a *quasi-automatic entitlement* of employers, whether public or private, to obtain and subsequently store sensitive health-related data (see §§ 85 – 86 of the judgment).

10. Other provisions of Instruction no. 165 stipulate that the employer has a duty to synchronise regularly the records with those of the military

---

[10] See *ibid.,* § 53 and *Z. v. Finland*, no. 22009/93, § 101, 25 February 1997, referring to *W. v. the United Kingdom*, 8 July 1987, § 64, Series A no. 121.

[11] Ruling of the Constitutional Court of Ukraine of 30 October 1997 in *K.G. Ustymenko*, case no. 18/203-97. See further references in §§ 25, 41 and 80 of the Chamber judgment.

[12] *Gardel v. France*, no. 16428/05, §§ 69-70, 17 December 2009.

enlistment offices and citizens have a duty to inform the competent authorities of any changes in their health status. The applicant's employer was able to access and use the old data without any prior assessment of whether that data would be "potentially decisive", "relevant" or "of importance" to the decision on the applicant's promotion.[13] The applicant repeated several times during the domestic proceedings that the data relied on was both outdated and imprecise. It would therefore appear that the impugned legislative framework did not provide procedures that adequately regulated the use and destruction of confidential data.[14]

11. The decisions of the domestic courts also seem to provide for the disclosure and use of data for purposes unrelated to the original purpose for its collection. Articles 2 and 153 of the Labour Code afforded the employer great discretion with regard to the use and disclosure of health-related data on the basis that employees shall be entitled to and employers shall create a healthy and safe working environment. The broad discretion thereby conferred on employers was not capable, without appropriate safeguards, of protecting sensitive data from being disseminated to and ultimately by third parties, such as the applicant's colleagues.[15]

12. In the light of the above considerations, we consider that the applicable Ukrainian rules which permitted, even mandated, the possession of information by employers relating to the grounds for dispensation from military service of its employees, were not formulated with sufficient precision regarding the retention, disclosure and use of health-related data, resulting in a lack of foreseeability. Neither did those rules describe and circumscribe with sufficient clarity the scope of the discretion conferred on the competent authorities and the manner in which that discretion had to be exercised. This centrality of (un)lawfulness to the Court's finding of a violation of Article 8 is evident in the content and construction of the judgment itself, with §§ 84 to 89 and § 91 referring repeatedly and clearly to issues which go to an absence of quality and a lack of foreseeability in the domestic legal framework.

13. We are not suggesting that it was not open to the Chamber to proceed to an analysis of necessity, transferring the concerns about the quality of the applicable law to that analysis. This is something which the Court has done on other occasions in Article 8 cases.[16] In addition, since

---

[13] *L.H. v. Latvia*, cited above, § 58; *M.S. v. Sweden*, no. 20837/92, §§ 38, 42 and 43, 27 August 1997; and *L.L. v. France*, no. 7508/02, § 46, ECHR 2006-XI.

[14] *L.H. v. Latvia*, cited above, § 50; *S. and Marper*, cited above, § 99; *Kruslin v. France*, 24 April 1990, §§ 33 and 35, Series A no. 176-A; *Rotaru v. Romania*, cited above, §§ 57-59; *Weber and Saravia v. Germany* (dec.), no. 54934/00, ECHR 2006-XI; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, §§ 75-77, 28 June 2007; and *Liberty and Others v. the United Kingdom*, no. 58243/00, §§ 62-63, 1 July 2008.

[15] *L.H. v. Latvia*, cited above, § 56.

Ukrainian data protection law has since been amended, the passage of time since the lodging of the applicant's case meant that concentrating on lawfulness would have led to the declaration of a purely historical violation of Article 8 without any guidance to national authorities and courts regarding how to comply in future with the principle of proportionality in similar cases which might arise under the new, amended legislation.

14. That being said, the passage of time must not alter the Court's identification of where the crux of the legal problem lies in any given case. In addition, the subsequent amendment of Ukrainian data protection rules constituted further proof, if indeed that was required, of a lawfulness problem at the material time. The Court has frequently recognised, as indicated previously, that domestic law may be couched in vague terms and that the interpretation and application of such terms are questions of practice. It is precisely the role of domestic courts to dissipate interpretational doubts and it is precisely that which the domestic courts had difficulty doing in the instant case, as is clear from the toing and froing between the Central District Court, the Court of Appeal and the Supreme Court.[17] Those courts themselves highlighted the shortcomings in the applicable domestic legislative framework, as did the Constitutional Court in the *Ustymenko* case referred to above.

15. Another reason for concentrating on the central problem of lawfulness in a case like this – albeit a purely pragmatic one – is the need for the Court, when possible, to itself act with the requisite degree of economy when faced with a choice of methodology. It has practised such restraint on other occasions when it has held that once it has examined the main legal questions raised in an application, there may be no need in the circumstances of a particular case to give a separate ruling on any remaining complaints.[18] With 75,250 applications pending before the Court, greater recourse to the "*Câmpeanu* technique", where possible, is likely to be of considerable benefit to applicants in the medium and long-term. In the instant case, not only did the Chamber, unnecessarily in our view, not concentrate on the central problem of lawfulness under Article 8 of the Convention, but it also proceeded to find a violation of Article 6 of the Convention due to the inadequacy of the response of the domestic courts to the applicants' complaints (see §§ 96-103 and 93 of the Chamber judgment). One of the factors examined in the context of necessity under Article 8 thus became the central and only plank of the examination under Article 6, despite the fact that the inadequacy of the domestic courts'

---

[16] See, for example, *S. and Marper*, cited above, § 99; and *Avilkina and Others v. Russia*, no. 1585/09, § 37, 6 June 2013, but contrast them with, for example, *M.M. v. the United Kingdom*, no. 24029/07, § 207, 13 November 2012.

[17] See *Delfi AS v. Estonia*, cited above, §§ 121-122; and *Kudrevičius and Others v. Lithuania* [GC], no. 37553/05, 110, 15 October 2015.

[18] See *Centre for Legal Resources on Behalf of Valentin Câmpeanu v. Romania* [GC], no. 47848/08, § 156, 17 July 2014, with further references.

response was, in any event, linked to the inadequacy of the domestic legal framework on which the Court should have concentrated in the first place. The identification of two separate violations which stemmed from the same problem was not, in our view, necessary.