



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

THIRD SECTION

CASE OF Y.G. v. RUSSIA

(Application no. 8647/12)

JUDGMENT

Art 8 • Private life • Positive obligations • Authorities' failure to adequately protect confidentiality of applicant's health data and to investigate its disclosure through a database being sold in a market

STRASBOURG

30 August 2022

FINAL

30/11/2022

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

In the case of Y.G. v. Russia,

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

Georges Ravarani, *President*,

Georgios A. Serghides,

María Elósegui,

Anja Seibert-Fohr,

Peeter Roosma,

Frédéric Krenc,

Mikhail Lobov, *judges*,

and Olga Chernishova, *Deputy Section Registrar*,

Having regard to:

the application (no. 8647/12) against the Russian Federation lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms (“the Convention”) by a Russian national, Mr Y.G. (“the applicant”), on 31 January 2012;

the decision to give notice of the application to the Russian Government (“the Government”);

the decision not to have the applicant’s name disclosed;

the parties’ observations;

Having deliberated in private on 24 May 2022 and 21 June 2022,

Delivers the following judgment, which was adopted on the last-mentioned date:

INTRODUCTION

1. The applicant complained that a database containing his health data had been available for sale at a market. He alleged that the database had belonged to the law-enforcement authorities, who had unlawfully collected, stored and entered his health data in it. He also complained that the authorities had failed to ensure the confidentiality of his data and to carry out an effective investigation into their disclosure.

THE FACTS

2. The applicant was born in 1971 and lives in Moscow. He was represented by Mr I. Sharapov, a lawyer practising in Moscow.

3. The Government were initially represented by Mr M. Galperin, former Representative of the Russian Federation to the European Court of Human Rights, and later by his successor in this office, Mr M. Vinogradov.

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

I. BACKGROUND TO THE CASE

5. The applicant is HIV-positive and suffers from hepatitis. He is registered with the Moscow Centre for the Prevention and Control of Aids.

6. In February 2011 an acquaintance of the applicant informed him that he had purchased, at Savelovskiy Market in Moscow, a database from which he had learnt of the applicant's conditions. In order to verify this information, the applicant purchased a compact disc containing a database from the same market.

7. On the first page of the database there was written in Russian "ЗИЦ Москва 02.2007". According to the applicant, the abbreviation "ЗИЦ" stood for *Зональный информационный центр Главного управления внутренних дел г. Москвы* – the Information Centre of the Moscow Department of the Interior ("the Information Centre"), and the database was dated 2007. The "Properties" dialog box indicated that copyright belonged to the company C.I.

8. The database consisted of a table divided into sections according to the type of personal data, such as first name, surname, place and date of birth, gender, ethnicity and address. It also contained specific types of information, such as nicknames, membership of organised criminal groups, criminal records and preventive measures applied, as well as a section entitled "date of entry".

9. The database contained data in respect of 213,355 people registered as living in Moscow; 203,604 people registered as living elsewhere but living in Moscow; and foreigners living in Moscow. It also contained information on 281 people with HIV, 30 people suffering from Aids and 750 people suffering from hepatitis.

10. The applicant was registered in the database under the number 308812. It contained the following information about him: (1) his name, patronymic and surname; (2) his date and place of birth; (3) his nationality; (4) his place of residence and address; and (5) his conviction for hooliganism, theft and unlawful possession of drugs. In the section entitled "Notes", it was stated that the applicant was "a hooligan, thief and drug addict, was suffering from Aids and hepatitis". In the section entitled "date of entry", the date 26 April 1999 was indicated.

11. In March 2011 the applicant's representative went to Savelovskiy Market to verify the information received from the applicant. Various databases allegedly belonging to different State agencies were available for sale, including a database similar to the one bought by the applicant. The applicant's representative purchased a copy of that database from a certain E., who provided him with his mobile telephone number in case he had problems opening the database on his computer.

II. COMPLAINT TO THE INFORMATION CENTRE OF THE MOSCOW DEPARTMENT OF THE INTERIOR

12. On 3 March 2011 the applicant complained to the Information Centre, asking it to clarify why its database contained information about his state of health; to remove the information about his having Aids, since it was untrue; and to remove the information about his hepatitis, since he had never consented to disclosure of that information. The applicant enclosed a printout of an extract from the database purchased at the market.

13. On 14 March 2011 the Information Centre replied that its database did not contain any information on the applicant's health and that the enclosed printout had nothing to do with its database.

III. COMPLAINTS TO THE INVESTIGATIVE COMMITTEE OF THE RUSSIAN FEDERATION

14. On 18 April 2011 the applicant complained to the Investigative Committee of the Russian Federation ("the Investigative Committee"). He alleged that a database entitled "Database of the Information Centre of the Moscow Department of the Interior" was being sold at Savelovskiy Market in Moscow. It contained personal data of people living in Moscow and the Moscow region, including data about his health and his HIV status. The applicant enclosed a printout of the database, the original CD version and a video-recording showing him purchasing it.

15. The applicant submitted that the uninhibited sale of such a database at the market was unlawful under Article 137 § 2 (breach of privacy) and Article 285 § 1 of the Criminal Code (abuse of office), and had become possible as a result of the transfer or sale of the database by officials of the Ministry of the Interior ("the Ministry") to third parties.

16. On 21 April 2011 the Investigative Committee replied that since the issues complained of were not within its competence, his complaint had been forwarded to the Prosecutor General. On 12 May 2011 the Prosecutor General forwarded it to the prosecutor of Moscow. On 25 May 2011 the prosecutor of Moscow forwarded it to the prosecutor of the Tverskoy District of Moscow.

17. On 1 June 2011 the prosecutor of the Tverskoy District replied that there was no evidence that any of the officials of the Moscow Department of the Interior had committed an offence. There was therefore no need to carry out a pre-investigation inquiry in accordance with Articles 144 and 145 of the Code of Criminal Procedure. In so far as his complaint concerned the fact that the database of the Information Centre was available at Savelovskiy Market, that market was not within the territorial jurisdiction of the prosecutor of the Tverskoy District.

18. On 23 January 2012 the applicant asked the Investigative Committee to clarify on what legal basis it had refused to conduct a pre-investigation

inquiry in connection with his report of a crime. It replied that the complaint did not contain enough information that would disclose elements of a crime.

19. By a final decision of 8 August 2011, the Moscow City Court dismissed a judicial complaint by the applicant against the Investigative Committee's failure to carry out a pre-investigation inquiry in respect of his report of a crime. The court established that on 18 April 2011 the applicant had lodged a criminal complaint with the Investigative Committee, which had examined it and concluded that it did not contain enough information indicating that a crime had been committed by officials of the Ministry.

IV. FURTHER DEVELOPMENTS

20. Shortly after submitting his complaints to the law-enforcement authorities, the applicant's representative was allegedly contacted by the Security Service of the Moscow Department of the Interior and invited to make a statement concerning the sale of the database at the markets of Moscow. The applicant's representative learnt from the Security Service that an inquiry was being conducted on the order of the Moscow Department of the Interior since information about the sale of the database of the Information Centre had appeared in the media.

21. In July 2013 the applicant allegedly purchased at Savelovskiy Market a database dating from 2010 similar to the one he had purchased in 2011. It contained the same information about his state of health, in addition to information about other people.

22. After notice of the application was given to the Government, the applicant learnt that on 15 March 1999, when he had been a suspect in criminal proceedings, the investigator in charge of the case had requested the Hospital for Infectious Diseases to provide information on his conditions. The applicant provided the Court with a copy of this request. The hospital allegedly replied that the applicant had been registered as having HIV and hepatitis.

V. PRESS ARTICLES

23. The applicant provided the Court with three news articles published on the websites vedomosti.ru (dated 14 June 2011), gazeta.ru (dated 28 June 2011) and interfax.ru (dated 4 October 2011). The Government did not contest the authenticity of those articles.

24. The article on vedomosti.ru shared information provided by the Russian telecoms regulator (Roskomnadzor) and the Ministry. According to those sources, in March 2011 Roskomnadzor and the Ministry had carried out a raid at Savelovskiy Market in Moscow, following which administrative-offence proceedings were initiated in respect of owners of market stalls. On 8 June 2011 Roskomnadzor and the Ministry had carried

out a raid on a shopping centre in Moscow and confiscated more than forty CDs containing databases allegedly belonging to the Ministry.

25. The article on gazeta.ru contained information provided by the Ministry's headquarters in Moscow. According to that information, the Ministry and the Federal Security Service had carried out a raid on three shopping centres in Moscow, including Savelovskiy Shopping Centre. They had confiscated more than fifteen thousand databases containing the personal data of Russian citizens.

26. The article on interfax.ru contained information provided by the Ministry's headquarters in Moscow. According to that information, the Moscow police had carried out an operation under the code name "Kontrafact", which had revealed the unlawful sale of databases of various State agencies, such as the Information Centre in Moscow. The databases all contained the personal data of citizens of the Russian Federation.

VI. CHECKS CARRIED OUT ON 10 OCTOBER 2017

27. According to the Government, on 10 October 2017 checks were carried out regarding the applicant's data stored in the Ministry's database. It was established that the only information stored therein was information concerning the applicant's criminal record.

RELEVANT LEGAL FRAMEWORK

I. RELEVANT DOMESTIC LAW

28. The Basic Principles of Public Health Law of the Russian Federation (FZ-5487 of 22 July 1993), as in force at the relevant time, provided as follows:

Section 61. Confidential medical information

"Information concerning a medical consultation, an individual's health, his or her diagnosis and other data obtained in the course of examination or treatment shall be considered confidential [medical information]. ...

Confidential medical information cannot be disclosed by [people] privy to it as a result of their studies or the performance of their professional or other duties, except as provided for in subsections (3) and (4) of this section.

A person or his legal representative may consent to the disclosure of confidential medical information to other persons, including officials, for the patient's examination and treatment, scientific research, publications, training and other purposes.

Confidential medical information may be disclosed without the consent of the individual or his legal representative:

...

3) at the request of investigating bodies, a prosecutor, or a court in connection with an investigation or judicial proceedings ...

Persons who have lawfully received confidential medical information may be held liable by way of disciplinary, administrative or criminal proceedings for the disclosure of this information, having regard to the damage caused ...”

Section 69. The individual’s right to appeal against actions of state bodies or officers infringing the individual’s rights and liberties in the public health sphere

“Actions of State bodies or officers which infringe the individual’s rights and liberties set forth in the present Basic Principles in the sphere of public health may be appealed against to higher State bodies or officials or to a court in accordance with the applicable legislation.”

29. Article 137 of the Criminal Code (FZ-63 of 13 June 2006), as in force at the relevant time, punished by a fine, correctional labour, a custodial sentence of up to four months or imprisonment of up to two years the unauthorised collection or dissemination of information about the private life of a person without his or her consent (Article 137 § 1). The same actions carried out by an official using his or her position were punishable by a fine, a ban on occupying certain positions, a custodial sentence of up to six months or imprisonment of up to four years (Article 137 § 2).

30. Article 13.11. of the Code of Administrative Offences (FZ-195 of 30 December 2001), as in force at the relevant time, provided that a breach of the statutory procedure for collecting, storing, processing or disseminating information about citizens (personal data) entailed a warning or the imposition of an administrative fine on citizens in the amount of three hundred to five hundred roubles, on officials in the amount of five hundred to one thousand roubles, and on legal entities in the amount of five thousand to ten thousand roubles.

II. RELEVANT COUNCIL OF EUROPE INSTRUMENTS

31. The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (“the Data Protection Convention” or “Convention 108”), of 28 January 1981, has entered into force in respect of the Russian Federation on 1 September 2013. Article 2 defines “personal data” as “any information relating to an identified or identifiable individual (“data subject”). The Data Protection Convention provides as follows:

“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;
- (e) 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.

Article 6 – Special categories of data

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

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 8 – Additional safeguards for the data subject

Any person shall be enabled:

- (a) to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file;
- (b) to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form;
- (c) to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention;
- (d) to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

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.”

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

32. The applicant complained under Articles 8 and 13 of the Convention that the law-enforcement authorities had unlawfully collected, stored and entered his health data in a database, and that they had failed to ensure the

confidentiality of his data and to carry out an effective investigation into their disclosure. The Court, being the master of the characterisation to be given in law to the facts of the case (see *Radomilja and Others v. Croatia* [GC], nos. 37685/10 and 22768/12, §§ 114 and 126, 20 March 2018), finds it appropriate to examine the applicant's complaints under 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.”

A. Admissibility

33. The Court reiterates that personal information relating to a patient belongs to his or her private life (see *I. v. Finland*, no. 20511/03, § 35, 17 July 2008). It is not in dispute between the parties that the database purchased by the applicant at the market contained a compilation of the applicant's personal data, including his health data. Therefore, the circumstances of the present case fall within the scope of the applicant's private life protected under Article 8 § 1 of the Convention.

34. The Court considers that the application is neither manifestly ill-founded nor inadmissible on any other grounds listed in Article 35 of the Convention. It must therefore be declared admissible.

B. Merits

1. The parties' submissions

(a) The applicant

35. The applicant submitted that according to registers held by the telecoms regulator Roskomnadzor, the Ministry was registered as a data operator. The applicant's health data had been registered in the Ministry's database in 1999, after the Hospital for Infectious Diseases had provided them to the investigator. The database purchased by the applicant at the market had belonged to the Ministry, since it contained information which could have been known only to the Ministry, such as his criminal record, and had been compiled by C.I., a company which collaborated with the law-enforcement authorities. The *prima facie* evidence provided by him together with the report of a crime had been enough to warrant the institution of criminal proceedings.

(b) The Government

36. The Government submitted that the law did not empower the Ministry to create and maintain databases concerning people with infectious or other diseases, except for data concerning people suffering from drug addiction. The Ministry had never used in its work the database management system C.I. referred to by the applicant, had never collected or stored the applicant's health data, and could not be held responsible for their disclosure.

37. The domestic law provided a legal framework for the protection of the applicant's private life (Articles 137, 272 and 285 of the Criminal Code, Article 13.11 of the Code of Administrative Offences and Article 152.2 of the Civil Code (introduced by FZ-142 of 2 July 2013)).

38. In 2011 the applicant had complained to the domestic authorities in accordance with Federal Law FZ-59 on the procedure for handling complaints by citizens of the Russian Federation. The authorities had examined his complaint and provided a reply. He had never lodged a criminal complaint under Articles 144 and 145 of the Code of Criminal Procedure. Between 2012 and 2017 the applicant had not lodged any complaints with the Ministry, nor had he informed it of the alleged purchase of another database in 2013.

39. It was impossible to confirm whether in 2011 the Ministry had carried out an inquiry into the sale of databases at the markets of Moscow. The archives of the Moscow Department of the Interior had been destroyed in 2016 on expiry of the statutory minimum storage period. In 2011 the Ministry had not confiscated any databases with citizens' health data at Savelovskiy Market.

2. The Court's assessment

(a) General principles

40. The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 of the Convention (see *Leander v. Sweden*, 26 March 1987, § 48, Series A no. 116, and *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 67, ECHR 2008).

41. The primary purpose of Article 8 is to protect against arbitrary interference by a public authority with a person's private and family life, home, and correspondence. Where the case concerns a negative obligation, the Court must assess whether the interference was consistent with the requirements of paragraph 2 of Article 8 – that is to say in accordance with the law, in pursuit of a legitimate aim, and necessary in a democratic society (see *Libert v. France*, no. 588/13, §§ 40 and 42, 22 February 2018).

42. In addition to this primarily negative undertaking, there may be positive obligations inherent in effective respect for private or family life (see *Bărbulescu v. Romania* [GC], no. 61496/08, § 108, 5 September 2017).

43. 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. There are different ways of ensuring respect for private life and the nature of the State's obligation will depend on the particular aspect of private life that is at issue. While the choice of the means to secure compliance with Article 8 in the sphere of protection against acts of individuals is, in principle, within the State's margin of appreciation, effective deterrence against grave acts, where fundamental values and essential aspects of private life are at stake, requires efficient criminal-law provisions and their application through effective investigation and prosecution (see *Ageyevy v. Russia*, no. 7075/10, §§ 195-96, 18 April 2013, and *Khadija Ismayilova v. Azerbaijan*, nos. 65286/13 and 57270/14, §§ 115-17, 10 January 2019).

44. The protection of personal data, particularly medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a person but also to preserve his or her confidence in the medical profession and in the health services in general. The domestic law must afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention (see *Z v. Finland*, 25 February 1997, § 95, *Reports of Judgments and Decisions* 1997-I; *M.S. v. Sweden*, 27 August 1997, § 41, *Reports* 1997-IV; and *L.H. v. Latvia*, no. 52019/07, § 56, 29 April 2014). The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned (see *S. and Marper*, cited above, § 103).

45. The above considerations are especially valid as regards protection of the confidentiality of information about a person's HIV infection. 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. For this reason, it may also discourage persons from seeking diagnosis or treatment and thus undermine any preventive efforts by the community to contain the pandemic. The interests in protecting the confidentiality of such information will therefore weigh heavily in the balance in determining whether the interference was proportionate to the legitimate aim pursued. Such interference cannot be compatible with Article 8 of the Convention unless it is justified by an overriding requirement in the public interest (see *Z v. Finland*, cited above, § 96).

(b) Application of the principles to the present case

46. The Court observes that the database purchased by the applicant at the market apparently contained personal data in respect of more than 400,000 people registered as living in Moscow and Moscow region, including the applicant. It was not contested by the Government that only authorities had access to most of those data, such as criminal records and preventive measures applied (see paragraphs 8-10 above). The Government have not contested either that in the context of criminal proceedings against him the investigator had sought information about the applicant's health condition from the Hospital for Infectious diseases (see paragraph 22 above).

47. The question of whether the Ministry of the Interior had compiled the database containing the applicant's health data together with other data is disputed by the parties (see paragraphs 35 and 36 above). However, in the context of the present case, there is no explanation other than that the State authorities, who had access to the data in question, had failed to prevent a breach of confidentiality, as a result of which that data had become publicly available, thus engaging the responsibility of the respondent State. The Court also notes that the circumstances of this major privacy breach have never been elucidated (see paragraphs 14-19 above and paragraph 51 below on the obligation to investigate). The Court has repeatedly stressed the importance of appropriate safeguards to prevent the communication and disclosure of health data (see the principles quoted in paragraph 44 above). The Court therefore finds that the authorities have failed to protect the confidentiality of the applicant's health data, also in breach of the relevant domestic provisions (see paragraphs 28-30 above).

48. Furthermore, whilst accepting that, regarding cases concerning alleged breach of privacy, a criminal-law remedy is not always required, and the civil law nature remedies could be seen as sufficient (see, *mutatis mutandis*, *Söderman v. Sweden* [GC], no. 5786/08, § 85, ECHR 2013), the Court observes that Article 152.2 of the Civil Code referred to by the Government was introduced by FZ-142 of 2 July 2013, that is after the applicant had introduced his application to the Court on 31 January 2012, and had therefore not been available to him prior to lodging his application.

49. The Court further observes that the applicant's allegations concerned the disclosure of his health data, as a part of the compilation of a vast amount of data and were supported by *prima facie* evidence. In the face of such a major privacy breach, in practical terms, the applicant acting on his own, without the benefit of the State's assistance in the form of an official inquiry, had no effective means of establishing the perpetrators of these acts, proving their involvement and bringing proceedings against them in the domestic courts. Accordingly, the Court cannot find that the complaint to the Investigative Committee was an inappropriate avenue of protection of his rights in the applicant's case.

50. It was established by the domestic courts that on 18 April 2011 the applicant had lodged a criminal complaint with the Investigative Committee. He informed the authorities that a database containing his health data, including his HIV status, had been available for purchase at a market. Despite this evidence, the investigative authorities and the courts consistently considered that there were no reasons to investigate as the information in question “did not disclose elements of a crime” (see paragraphs 14-19 above).

51. The Court observes that Article 137 of the Criminal Code (see paragraph 29 above) provided a legal framework for prosecuting intrusion into one’s private life and it cannot be said that the investigation could not be opened because of any deficiency either in the legislative framework or in domestic practice, or that there were any other circumstances objectively precluding the investigation authority from swiftly launching an investigation and proceeding to the collection of evidence and the identification of those responsible. However, the authorities never investigated the matter.

52. Having regard to the above, the Court finds that the authorities failed to comply with their positive obligation to ensure adequate protection of the applicant’s right to respect for his private life. There has accordingly been a violation of Article 8 of the Convention in that respect.

53. In view of this finding, the Court does not deem necessary to consider the remainder of the applicant’s complaint that the State authorities had allegedly unlawfully collected, stored and entered his health data in a database.

II. APPLICATION OF ARTICLE 41 OF THE CONVENTION

54. 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

55. The applicant claimed 25,000 euros (EUR) in respect of non-pecuniary damage.

56. The Government contested this claim.

57. The Court awards the applicant EUR 7,500 in respect of non-pecuniary damage, plus any tax that may be chargeable.

B. Costs and expenses

58. The applicant also claimed EUR 4,260 for the costs and expenses incurred before the domestic courts and for those incurred before the Court.

59. The Government contested this claim.

60. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown that these were actually and necessarily incurred and are reasonable as to quantum. In the present case, regard being had to the documents in its possession and the above criteria, the Court considers it reasonable to award the sum of EUR 2,000 covering costs under all heads, plus any tax that may be chargeable to the applicant.

C. Default interest

61. 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 application admissible;
2. *Holds* that there has been a violation of Article 8 of the Convention;
3. *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, the following amounts, to be converted into the currency of the respondent State at the rate applicable at the date of settlement:
 - (i) EUR 7,500 (seven thousand five hundred euros), plus any tax that may be chargeable, in respect of non-pecuniary damage;
 - (ii) EUR 2,000 (two thousand euros), plus any tax that may be chargeable to the applicant, in respect of costs and expenses;
 - (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amounts at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;
4. *Dismisses* the remainder of the applicant's claim for just satisfaction.

Done in English, and notified in writing on 30 August 2022, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Olga Chernishova
Deputy Registrar

Georges Ravarani
President