Published in the USA
Zhurnal grazhdanskogo i ugolovnogo prava
Has been issued since 2014.
E-ISSN: 2413-7340
2022. 8(1): 23-29

DOI: 10.13187/zngup.2022.1.23
https://zgup.cherkasgu.press


# Personal Data Protection in European Court of Human Rights' Case Law

Olena V. Tarasenko [a] , [*]

[a] Emarket Ukraine, Ukraine

**Abstract**

Protecting personal data is one of the essential areas of development of modern jurisprudence. Personal data is closely related to a person's private life; their collection or disclosure may violate fundamental human rights. In addition, according to the Association Agreement between Ukraine and the EU, Ukraine must bring its legislation on protecting personal data closer to European standards. The status of a candidate country for joining the EU also imposes on Ukraine the obligation to get its ruling on protecting personal data closer to EU law.

Many acts deal with the legal regulation of personal data protection, both at the level of the Council of Europe and in the European Union. This paper focuses mainly on the relationship between personal data protection and human rights; therefore, the main emphasis is on studying the European Court of Human Rights practice.

The analysis of several ECtHR judgements (mostly from 2021–2022) made it possible to highlight several main trends:

Protecting personal data remains an important area of privacy protection.

In its decisions, the ECtHR seeks to establish criteria for balancing private and public interests in the context of personal data protection.

The practice of the ECtHR can be used to bring Ukrainian law and practice on protecting personal data closer to European standards.

**Keywords:** personal data, protection of personal data, the practice of the European Court of Human Rights, General Data Protection Regulation.

## 1. Introduction

Protecting personal data is one of modern science's most critical research areas. At the same time, creating effective personal data protection mechanisms is a subject of interest in jurisprudence and sociology, political science, marketing, data science, etc. Such complex and multi-disciplinary interest is due to the role played by personal data in modern society.

For Ukraine, the issue of personal data protection is of particular relevance. For example, Article 15 of the Association Agreement between Ukraine and the EU provides that «the parties have agreed to cooperate to ensure an adequate level of personal data protection in accordance with the highest European and international standards, in particular, relevant documents of the Council of Europe» (Association Agreement..., 2014). However, at present, progress in this area can be assessed as insignificant. According to the Action Plan for the implementation of the Association Agreement between Ukraine, on the one hand, and the European Union, the European

[*] Corresponding author
E-mail addresses: olena.tarasenko@olx.com (O. Tarasenko)

Atomic Energy Community and their member states, on the other hand, the legislation of Ukraine was to be brought into line with the EU legislation by May 25, 2020 (Plan of measures..., 2017). These measures were not implemented (Pulse of the Agreement..., 2022). On June 7, 2021, a draft law on the protection of personal data (draft law 5628) was submitted to the Verkhovna Rada of Ukraine, which, however, was never adopted (Draft Law..., 2021). On October 25, 2022, the draft law 8153 was submitted to the parliament, which at the time of writing this research is still being processed (Draft Law..., 2022).

However, personal data protection is not limited to legislative measures only. The law enforcement practice of both national and international courts, as well as the policies of large companies, also have a significant impact on the general security of personal data in Ukraine (Index..., 2022). Therefore, studying the materials of the law enforcement practice of the Court of the EU and the European Court of Human Rights can be helpful for the formation of legislative proposals and company policies and for developing common positions of national courts in Ukraine.

## 2. Materials and methods

The main sources for writing this paper became the acts of international law, case-law of European Court of Human Rights, documents of Parliamentary Assembly of Council of Europe, Committee of Ministers of Council of Europe, European Union, Ukrainian national legislation, and materials of the scientific publications.

The study used the basic methods of cognition: the historical and situational, formal-legal and the method of comparative law. The use of historical and situational method allows to understand the evolution of personal data protection mechanism. The formal-legal method was used to analyze official documents and case law on personal data protection in Europe. Method of comparative law defines the difference in models of personal data protection in different areas of data using.

## 3. Discussion

The Law of Ukraine «On the Protection of Personal Data» provides that personal data is information or a set of information about a natural person who is identified or can be specifically identified (Law, 2010).

The main act that defines the principles of working with personal data in the EU is Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). According to the article 4 GDPR, 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. The researchers emphasize that in the category of personal data, special (sensitive) data can also be distinguished, which include personal data on: racial or ethnic origin; political, religious or ideological beliefs; membership in political parties and trade unions; criminal conviction; health, sex life; biometric or genetic data (Bem, Horodyskyi, 2021). Also, the preamble of this document states that the protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her (Regulation..., 2016). This provision additionally emphasizes the importance of protecting personal data under current conditions and its connection with fundamental human rights.

Instead, for the Council of Europe, the actual act on the protection of personal data is the Convention for the protection of individuals with regard to the processing of personal data (Convention 108 +). This document also defines the concept of «personal data», which means any information relating to an identified or identifiable individual (Convention..., 1981). Article 4 of Convention 108+ provides that each Party shall take the necessary measures in its law to give effect to the provisions of this Convention and secure their effective application (Convention..., 1981).

The Parliamentary Assembly of the Council of Europe and the Committee of Ministers of the Council of Europe also did not stand aside from improving personal data protection. Thus, one of the first acts that proclaimed the need to protect personal data was Recommendation 509 (1968) PACE Human rights and modern scientific and technological developments. In it, the PACE declared that personal data directly connects with human rights.

The development of technologies and media necessitated the adoption of new acts related to protecting personal data. Among the documents of PACE, one can highlight, in particular, Resolution 22 on the protection of privacy of individuals vis-à-vis electronic data banks in the private sector (1973), Resolution 29 on the protection of individuals vis-à-vis electronic data banks in the public sector (1974), Resolution 721, Data processing and the protection of human rights (1980), Resolution 1604, Video surveillance of public areas (2008) and Resolution 1797, The need for a global consideration of the human rights implications of biometrics (2011). Among recent documents, attention is drawn to Resolution 1843 (2011). The protection of privacy and personal data on the Internet and online media and Resolution 1986 (2014) Improving user protection and security in cyberspace. In particular, the first states that the right to protection of privacy and personal data is a fundamental human right, which imposes on states the obligation to provide an adequate legal framework for such protection against interference by public authorities as well as by private individuals and entities. The authors of the resolution also emphasize that everyone must be able to control the use of their personal data by others, including any accessing, collection, storage, disclosure, manipulation, exploitation or other processing of personal data, with the exception of the technically necessary or lawful retention of ICT traffic data and localisation data; the control of the use of personal data shall include the right to know and rectify one's personal data and to have erased from ICT systems and networks all data which were provided without legal obligation (Resolution..., 2011).

The second resolution provides that everyone's private life, correspondence and personal data must be protected online; users shall always have the possibility to withdraw data, content and information; interception, surveillance, profiling or storage of user data by public authorities, commercial entities or private persons is only permissible where allowed by law in accordance with Article 8 of the European Convention on Human Rights; member States have a positive obligation to ensure adequate legal protection against the interception, surveillance, profiling and storage of user data; personal data archives must be subject to precautionary measures to protect them from data theft and fraud (Resolution..., 2014).

The Committee of Ministers of the Council of Europe is also involved in the topic of personal data protection. For example, in Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data, the Committee of Ministers declared that the data must be processed in a transparent, lawful and fair manner (Recommendation..., 2019). The provisions of Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment indicate that respect for human dignity, privacy and the protection of personal data should be safeguarded in the processing of personal data for employment purposes, notably to allow for the free development of the employee's personality as well as for possibilities of individual and social relationships in the workplace (Recommendation..., 2015).

Other acts of the Committee of Ministers also concern the protection of personal data in medicine, in general on the Internet, telephone services, during the provision of public services, etc. Separate recommendations are also devoted to the protection of the personal data of minors.

## 4. Results

However, the cases considered by the European Court of Human Rights are of most significant interest to our research. One of the first in this area was the case «Klass and others v. Germany», in which five German lawyers complained about excessive state interference in their privacy. In its decision, the European Court of Human Rights once again emphasized the need to comply with the requirement of proportionality of the interference with privacy (Case of Klass..., 1978).

The more recent practice of the Court shows the relevance of personal data protection, at least in such contexts as the collection of personal data, storage and use of personal data, and disclosure of personal data.

The collection of personal data and the consequences that such may lead to were discussed in the case of Florindo de Almeida Vasconcelos Gramaxo v. Portugal. The applicant complained that his employer installed a geolocation tracking device on his company vehicle. Ultimately, based on the data from this device, the applicant was dismissed from his job, depriving him of his livelihood. In the decision, the Court recalled that under Article 8 of the Convention, member states are subject to negative and positive obligations. Under certain circumstances, compliance with the positive obligations imposed by Article 8 requires the State to adopt a legislative framework capable of protecting the relevant right (§ 108) (Case of Florindo..., 2022). Based on the previous case law, the Court emphasized that national courts must take into account the following factors when balancing the various interests at stake:

i) Was the employee correctly informed about the possibility that the employer will take monitoring measures?

ii) What was the extent of the employer's surveillance and the degree of intrusion into the private lives of employees?

iii) Did the employer legitimately justify the use and extent of surveillance?

iv) Could a surveillance system be established based on less burdensome means and measures?

v) What were the surveillance's consequences for the employee exposed to it?

vi) Were adequate safeguards offered to the employee, especially when the employer's surveillance measures interfered with the individual's private life? (§ 109) (Case of Florindo..., 2022).

Since the employer duly informed the applicant of the installation of the geolocation device and the consequences of the use of the data collected by this device, as well as in view of the balancing by the national court of the interests of the applicant and the employer, the Court found that in the applicant's case, the interference did not constitute a violation of Article 8 Conventions (Case of Florindo..., 2022).

In the case of Y.G. v. Russia, the collection, storage and dissemination of information (including medical information) by internal affairs bodies were considered. The applicant, who has HIV and hepatitis, was informed that a database disk could be purchased at one of the markets in Moscow. This database, which was probably created by the internal affairs authorities, contained a table with the names of almost 500,000 people. The table included such data 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» (§ 8) (Y.G., 2022). 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 (§ 10) (Y.G., 2022).

The applicant appealed to the internal affairs authorities with a request to remove information about his health from the relevant database. The Information Center 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. The court emphasized that 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 (§ 44) (Y.G., 2022). Reflecting on the origins of the database, the Court emphasized that 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 (§ 47). Accordingly, the Court established a violation of Article 8 of the Convention (Y.G., 2022).

In the case of Centrum för rättvisa v. Sweden, the applicant complained that for a long time all his company's correspondence (by telephone, fax and e-mail) was or could be monitored by national intelligence, despite the sensitive content of such correspondence. The case is notable for developing the criteria used by the Court to assess the propriety of interference (Centrum..., 2021). More specifically, in addressing jointly «in accordance with the law» and «necessity» as is the established approach in this area, the Court will examine whether the domestic legal framework clearly defined:

- The grounds on which bulk interception may be authorised;
- The circumstances in which an individual's communications may be intercepted;
- The procedure to be followed for granting authorisation;
- The procedures to be followed for selecting, examining and using intercept material;
- The precautions to be taken when communicating the material to other parties;
- The limits on the duration of interception, the storage of intercept material and the circumstances in which such material must be erased and destroyed;
- The procedures and modalities for supervision by an independent authority of compliance with the above safeguards and its powers to address non-compliance;
- The procedures for independent ex post facto review of such compliance and the powers vested in the competent body in addressing instances of non-compliance (§ 275) (Centrum..., 2021).

Cases concerning the disclosure of personal data during investigations or public hearings are also quite indicative. Engaging in this context is the case of Panteleyenko v. Ukraine. Information about the applicant's mental health was disclosed in court proceedings. In assessing the relevant situation, the Court has traditionally applied a three-part test (whether the intervention was carried out «in accordance with the law», for a «legitimate aim» and whether it was «necessary in a democratic society»). The Court recalls that the phrase «in accordance with the law» requires that the measure complained of must have some basis in domestic law. It is to be noted that the Court of Appeal, having reviewed the case, came to the conclusion that the first instance judge's treatment of the applicant's personal information had not complied with the special regime concerning collection, retention, use and dissemination afforded to psychiatric data. Moreover, the Court notes that the details in issue being incapable of affecting the outcome of the litigation (i.e. the establishment of whether the alleged statement was made and the assessment whether it was libellous), the first instance request for information was redundant, as the information was not «important for an inquiry, pre-trial investigation or trial», and was thus unlawful for the purposes of Article 6 of the Psychiatric Medical Assistance Act 2000 (§ 60-61). Accordingly, the ECtHR found a violation of Article 8 of the Convention (Case of Panteleyenko..., 2006).

In the case of Algirdas Butkevicius v. Lithuania, the applicant is a former prime minister. During his tenure, a telephone conversation occurred between him and his colleague. As it turned out later, the colleague's phone was tapped by law enforcement agencies in connection with the anti-corruption proceedings against him. During public hearings in the parliament, the content of the conversation was made public. The applicant complained that the disclosure to the media of the transcripts of his telephone conversation had infringed his right to respect for his correspondence and had affected his right to respect for his private life. Initially, the applicant could not have known that his telephone conversation was being intercepted. Moreover, he had never been warned or even suspected that the transcripts of such a conversation would later be disclosed to the public, without any warning or grounds (§ 65-66) (Case of Algirdas Butkevicius, 2022). Having assessed the circumstances of the case, the Court decided that with regard to the applicant establishing and maintaining relationships with others, the Court finds that even if his reputation among his colleagues was affected by the disclosure of his telephone conversation, there are no factual grounds, let alone evidence, which he has put forward that would indicate that such an effect was so substantial as to have constituted a disproportionate interference with his rights guaranteed by Article 8 of the Convention (§ 102) (Case of Algirdas Butkevicius, 2022).

In Standard Verlagsgesellschaft mbH v. Austria (no. 3), the applicant was the company that owns the web forum. On this forum, users were recommended to register by leaving some personal data. According to the general rules, these data should not have been publicly available. In connection with certain events, a discussion took place on the forum in which insulting and

defamatory statements were made. The individuals referred to in the comments demanded that the applicant company remove the comments and disclose user data so that criminal or civil proceedings could be initiated against them. The applicant company deleted comments but did not provide data about forum users. Ultimately, the national court ordered the applicant company to disclose the relevant data (Case of Standard..., 2021).

In this regard, the court emphasized that in the light of the Declaration on freedom of communication on the Internet adopted by the Committee of Ministers of the Council of Europe, which emphasises the principle of anonymity for Internet users in order to enhance the free expression of opinions, information and ideas, the Court has no doubt that an obligation to disclose the data of authors of online comments could deter them from contributing to debate and therefore lead to a chilling effect among users posting in forums in general (§ 74) (Case of Standard..., 2021). The Court observes that different degrees of anonymity are possible on the Internet. An Internet user may be anonymous to the wider public while being identifiable by a service provider through an account or contact data that may be either unverified or subject to some kind of verification. A service provider may also allow an extensive degree of anonymity for its users, in which case users are not required to identify themselves at all and they may only be traceable – to a limited extent – through the information retained by Internet access providers. The release of such information would usually require an injunction by the investigative or judicial authorities and would be subject to restrictive conditions. It may nevertheless be required in some cases in order to identify and prosecute perpetrators (§ 77) (Case of Standard..., 2021).

However, even a prima facie examination requires some reasoning and balancing. In the instant case, the lack of any balancing between the opposing interests overlooks the function of anonymity as a means of avoiding reprisals or unwanted attention and thus the role of anonymity in promoting the free flow of opinions, ideas and information, in particular if political speech is concerned which is not hate speech or otherwise clearly unlawful. In view of the fact that no visible weight was given to these aspects, the Court cannot agree with the Government's submission that the Supreme Court struck a fair balance between opposing interests in respect of the question of fundamental rights (§ 95) (Case of Standard..., 2021).

## 5. Conclusion

Summing up the decisions of the European Court of Human Rights analyzed above, several trends can be pointed out.

First, cases in which the state's obligation to ensure adequate personal data protection is discussed in one way or another maintain their relevance. Given the development of information technologies and the emergence of new services that process users' personal data, the protection of personal data is becoming a subject of increasing concern.

Secondly, Article 8 of the Convention can be an effective tool for protecting personal data in the context of their connection with human rights. Currently, the ECtHR is following the path of distinguishing specific directions in work with personal data and establishing criteria for balancing private and public interests in the mentioned field. In this paper, we have considered examples of privacy violations through the collection, processing, storage and disclosure of personal data in medicine, fighting crime, ensuring national security, etc. In each case, the Court indicated the decisive circumstances for judgement establishment.

Thirdly, for EU member states, legislation in the field of personal data protection has become relatively unified because there is a fundamental EU act that defines the principles of regulation in this area. However, for other member states of the Council of Europe, protecting personal data at the level of legislation and policies of large companies is still challenging. Therefore, the perception of the EU member states' experience and the European Court of Human Rights practice can be a reference for developing legislative acts and ensuring the consistency of judicial and administrative practice.

## References

Association Agreement..., 2014 – Association Agreement between Ukraine and the EU (2014) (In Ukrainian). [Electronic resource]. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text

Bem, Horodyskyi, 2021 – *Bem, M., Horodyskyi, I.* (2021). Zakhyst personalnykh danykh: pravove rehuliuvannia ta praktychni aspekty [Personal Data Protection: legal regulation and practical aspects]. Council of Europe, 160 p. [in Ukrainian]

Case of Algirdas Butkevicius, 2022 – Case of Algirdas Butkevicius v. Lithuania, judgement of 14 June 2022. European Court of Human Rights. [Electronic resource]. URL: https://hudoc.echr.coe.int/eng?i=001-217713

Case of Florindo..., 2022 – Case of Florindo de Almeida Vasconcelos Gramaxo v. Portugal, judgement of 13 December 2022. European Court of Human Rights. [Electronic resource]. URL: https://hudoc.echr.coe.int/eng?i=001-221474

Case of Klass..., 1978 – Case of Klass and others v. Germany, judgement of 6 September 1978 . European Court of Human Rights. [Electronic resource]. URL: https://hudoc.echr.coe.int/eng?i=001-57510

Case of Panteleyenko..., 2006 – Case of Panteleyenko v. Ukraine, judgement of 29 June 2006. European Court of Human Rights. [Electronic resource]. URL: https://hudoc.echr.coe.int/eng?i=001-76114

Case of Standard..., 2021 – Case of Standard Verlagsgesellschaft mbH v. Austria (no. 3), judgement of 7 December 2021. European Court of Human Rights. [Electronic resource]. URL: https://hudoc.echr.coe.int/eng?i=001-213914

Centrum..., 2021 – Case of Centrum för rättvisa v. Sweden, judgement of 25 May 2021. European Court of Human Rights. [Electronic resource]. URL: https://hudoc.echr.coe.int/eng?i=001-210078

Convention..., 1981 – Convention 108 + Convention for the protection of individuals with regard to the processing of personal data. 1981. [Electronic resource]. URL: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

Draft Law..., 2021 – Draft Law on Personal Data Protection (2021) N 5628. [Electronic resource]. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=72160

Draft Law..., 2022 - Draft Law on Personal Data Protection (2022) N 8153. [Electronic resource]. URL: https://itd.rada.gov.ua/billInfo/Bills/Card/40707

Index..., 2022 – Index Of Personal Data Protection Report. 2022. [Electronic resource]. URL: https://uadigital.report/index-of-personal-data-protection-2021-eng.pdf

Law..., 2010 – Law on Personal Data Protection. № 2297-VI. [Electronic resource]. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

Plan of measures..., 2017 – Plan of measures for the implementation of the Association Agreement between Ukraine, on the one hand, and the European Union, the European Atomic Energy Community and their member states, on the other hand (2017) № 1106 [Electronic resource]. URL: https://zakon.rada.gov.ua/laws/show/1106-2017-%D0%BF#Text [in Ukrainian]

Pulse of the Agreement..., 2022 – Pulse of the Agreement. Monitoring the implementation of the plan of measures for the implementation of the Agreement. 2022. [Electronic resource]. URL: https://pulse.kmu.gov.ua/ua/streams/human-rights-justice-and-anticorupption/2020-substream5-95 [in Ukrainian]

Recommendation..., 2015 – Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment. [Electronic resource]. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a

Recommendation..., 2019 – Recommendation CM/Rec(2019)2 of the Committee of Ministers to member States on the protection of health-related data [Electronic resource]. URL: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168093b26e

Regulation..., 2016 – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). [Electronic resource]. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

Resolution..., 2011 – Resolution 1843 (2011). The protection of privacy and personal data on the Internet and online media [Electronic resource]. URL: https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=18039&lang=en

Resolution..., 2014 – Resolution 1986. Final version Improving user protection and security in cyberspace, 2014. [Electronic resource]. URL: https://pace.coe.int/en/files/20791/html

Y.G., 2022 – Case of Y.G. v. Russia, judgement of 30 August 2022. European Court of Human Rights. [Electronic resource]. URL: https://hudoc.echr.coe.int/eng?i=001-218920