PROTECTION OF HEALTH RELATED DATA AND PRIVACY RIGHTS

RALUCA BERCEA

ASSOCIATE PROFESSOR, LAW FACULTY, TIMISOARA

PROTECTION OF HEALTH RELATED DATA AND PRIVACY RIGHTS

PLAN:

1. Introduction
2. European Data Protection Law – background and concepts
3. Health Data – the concept
4. The system of protection. Additional safeguards and guarantees
5. Anonymisation and pseudoanonymisation
6. Electronic health records
7. Practical illustrations

1. INTRODUCTION: HEALTH RELATED DATA - PRINCIPLES OF PROTECTION IN A NUTSHELL

Key principles of data protection:

- 1. lawful, transparent and fair processing;
- 2. purpose limitation;
- 3. data minimisation;
- 4. accuracy;
- 5. storage limitation;
- 6. security;
- 7. accountability

General principle of European law: certain categories of data require special protection*

Medical data

- among the most sensitive data (as they can reveal a higher degree of an individual's privacy, intimate life, individual characteristics, personality)
- stricter protection [Art. 9 GDPR, Art. 6 MC108]

General prohibition [processed for specific purposes and under specific conditions]

1. INTRODUCTION: HEALTH RELATED DATA - PRINCIPLES OF PROTECTION IN A NUTSHELL

Special derogations:

- informed and specific consent of the data subject
- by health professionals for specific purposes
- for the interest of the data subject

Member States: own derogations, including limitations or futher conditions, in line with the European principles

* EXTENT OF PROTECTION

The applicant's ex-husband, who was infected with HIV, had committed a number of sexual offences. He was subsequently convicted of manslaughter on the ground that he had knowingly exposed his victims to the risk of HIV infection. The national court ordered the full judgment and the case documents to remain confidential for 10 years despite requests from the applicant for a longer confidentiality period. The appellate court refused these requests, and its judgment contained the full names of both the applicant and her ex-husband *(*ECtHR, *Z. v. Finland, 1997)*

1. INTRODUCTION: HEALTH RELATED DATA - RIGHT TO RESPECT FOR PRIVATE LIFE IN A NUTSHELL

"**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 European Convention on Human Rights, which guarantees the right to respect for private and family life, home and correspondence] ... **The subsequent use of the stored information has no bearing on that finding** ... However, **in determining whether the personal information retained by the authorities involves any ... private-life** [aspect] ..., **the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained** ..." (*S. and Marper v. the United Kingdom*, 2008)

An illustration -

The applicant alleged that the collection of her personal medical data by a State agency without her consent had violated her right to respect for her private life.

1. INTRODUCTION: HEALTH RELATED DATA - RIGHT TO RESPECT FOR PRIVATE LIFE IN A NUTSHELL

"The Court recalled **the importance of the protection of medical data to a person's enjoyment of the right to respect for private life**. It held that there had been a violation of Article 8 of the Convention in the applicant's case, finding that **the applicable law had failed to indicate with sufficient clarity the scope of discretion conferred on competent authorities and the manner of its exercise**. The Court noted in particular that Latvian law in no way limited the scope of private data that could be collected by the state agency, which resulted in it collecting medical data on the applicant relating to a seven-year period indiscriminately and without any prior assessment of whether such data could be potentially decisive, relevant or of importance for achieving whatever aim might have been pursued by the inquiry at issue.

(ECtHR, *L.H. v. Latvia*, 2014)

2. EUROPEAN DATA PROTECTION LAW – BACKGROUND THE RIGHT TO DATA PROTECTION

EUROPEAN UNION LAW

- Treaty on the Functioning of the European Union, Article 16
- Charter of Fundamental Rights of the European Union (the Charter), Article 8 (right to protection of personal data)
- Regulation (EU) 2016/679 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*), OJ 2016 L 119

COUNCIL OF EUROPE

- ECHR, Article 8 (right to respect for private and family life, home and correspondence)
- Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Modernised Convention 108)
- Recommendation No. R (97) 5 on the Protection of medical data, updated by the recommendation on the Protection of Health-Related Data

2. EUROPEAN DATA PROTECTION LAW – BACKGROUND LIMITATIONS ON THE RIGHT TO PROTECTION OF PERSONAL DATA

EUROPEAN UNION LAW

The Charter, Article 52 (1)

General Data Protection Regulation, Article 23

CJEU, Joined cases C-92/09 and C-93/09, Volker und Markus Schecke GbR and Hartmut Eifert v. Land Hessen [GC], 2010

COUNCIL OF EUROPE

ECHR, Article 8 (2)

Modernised Convention 108, Article 11 ECtHR, S. and Marper v. the United Kingdom [GC], Nos. 30562/04 and 30566/04, 2008

2. EUROPEAN DATA PROTECTION LAW – BACKGROUND THE RIGHT TO DATA PROTECTION

COUNCIL OF EUROPE

• Under Article 8 of the ECHR, **a person's right to protection with respect to the processing of personal data forms part of the right to respect for private and family life, home and correspondence**.

• CoE Convention 108 is the first and, to date, the only international legally binding instrument dealing with data protection. The Convention underwent a modernisation process, completed with the adoption of amending Protocol CETS No. 223.

EUROPEAN UNION LAW

• Under EU law, **data protection has been acknowledged as a distinct fundamental right**. It is affirmed in Article 16 of the Treaty of the Functioning of the EU, as well as in Article 8 of the EU Charter of Fundamental Rights.

• Under EU law, data protection was regulated for the first time by the Data Protection Directive in 1995.

• In view of rapid technological developments, the EU adopted new legislation in 2016 to adapt data protection rules to the digital age. The General Data Protection Regulation became applicable in May 2018, repealing the Data Protection Directive.

2. EUROPEAN DATA PROTECTION LAW – CONCEPTS

The right to respect for private life and the right to the protection of personal data

- closely related, protect similar values [the autonomy and human dignity of individuals]
- are an essential prerequisite for the exercise of other fundamental freedoms

The right to respect for private life and the right to the protection of personal data

THE RIGHT TO RESPECT FOR PRIVATE LIFE **consists of a general prohibition on interference, subject to some public interest criteria that can justify interference in certain cases**.

- THE PROTECTION OF PERSONAL DATA - **a modern and active right, putting in place a system of checks and balances to protect individuals whenever their personal data are processed**. The **processing** must comply with the essential components of personal data protection: **independent supervision and the respect for the data subject's rights. It must be fair, for specified purposes, and based on either the consent of the person concerned or a legitimate basis laid down by law**. Individuals **must have the right to access their personal data and to have it rectified, and compliance with this right must be subject to control by an independent authority**.

2. DATA PROTECTION CF. PRIVATE LIFE. CONCEPTS

The right to personal data protection:

- comes into play whenever personal data are processed
- it is broader than the right to respect for private life
- any processing operation of personal data is subject to appropriate protection.

Data protection concerns all kinds of personal data and data processing, irrespective of the relationship and impact on privacy. Processing of personal data may also infringe on the right to private life. However, it is not necessary to demonstrate an infringement on private life for data protection rules to be triggered. The right to privacy concerns situations where a private interest, or the "private life" of an individual, has been compromised.

The concept of "private life": broadly interpreted in the case law, as covering intimate situations, sensitive or confidential information, information that could prejudice the perception of the public against an individual, and even aspects of one's professional life and public behaviour.

The assessment of whether or not there is, or has been, an interference with "private life" depends on the context and facts of each case. **By contrast**, **any operation involving the processing of personal data could fall under the scope of data protection rules and trigger the right to personal data protection**.

e.g: where an employer records information relating to the names of and remuneration paid to employees, the mere recording of this information cannot be regarded as an interference with private life. Such an interference could, however, be argued if, for instance, the employer transferred the employees' personal information to third parties. Employers must in any case comply with data protection rules because recording employees' information constitutes data processing.

3. HEALTH DATA. THE CONCEPT

- all personal data concerning health of an individual, including genetic and biometric data [art. 9 GDPR, art. 6 C 108] and data that have a clear and close link with health
- health related data: all personal data concerning the physical and mental health of an individual, including the provision of health care services, which reveals information about the individual's past, current or future health
- health goes beyond the doctor/patient relationship, covering any person likely to keep health data
- all data contained in medical documentation, in electronic health records and in electronic health record systems should be considered to be sensitive data

4. THE SYSTEM OF PROTECTION. ADDITIONAL SAFEGUARDS AND GUARANTEES THE CoE MEDICAL DATA RECOMMENDATION

4.1. The CoE Medical Data Recommendation of 1997 applies the principles of Convention 108 to data processing in the medical field.

Key elements: the legitimate purposes of processing medical data, the necessary professional secrecy obligations of persons using health data, and the rights of the data subjects to transparency and access, rectification and deletion.

Medical data which are lawfully processed by healthcare professionals may not be transferred to law enforcement authorities unless "sufficient safeguards to prevent disclosure inconsistent with the respect for [...] private life guaranteed under Article 8 of the ECHR" are provided.

The national law must also be "formulated with sufficient precision and afforded adequate legal protection against arbitrariness".

Special provisions on the medical data of unborn children and incapacitated persons, and on the processing of genetic data. Scientific research is explicitly acknowledged as a reason for conserving data longer than they are needed, although this will usually require anonymisation.

4. THE SYSTEM OF PROTECTION. ADDITIONAL SAFEGUARDS AND GUARANTEES THE GDPR

4.2. Article 9 (1) of the General Data Protection Regulation

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and **the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited**.

UNLESS: THE DATA SUBJECT GIVES HER/HIS EXPLICIT CONSENT OR THE PROCESSING MEETS ONE ADDITIONAL REQUIREMENT (e.g.): when the data is manifestly made public by the subject; when processing is necessary for the establishment, exercise or defense of legal claims or whenever courts are acting in their judicial capacity; legitimate activities of NGO's; processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

Additionally: article 9 (2) (h) of the General Data Protection Regulation allows for processing medical data **(a)** where this is required for the purposes of preventative medicine, medical diagnosis, the provision of care or treatment, or the management of healthcare services. Processing is permissible, however, **(b)** only where performed by a healthcare professional subject to an obligation of professional secrecy, or by another person subject to an equivalent obligation.

4. THE SYSTEM OF PROTECTION. ADDITIONAL SAFEGUARDS AND GUARANTEES THE GDPR

4.2. Article 9 (2) of the General Data Protection Regulation (e.g.)

CONSENT: explicit; can only be an appropriate legal basis if the data subject is offered both control and a genuine choice with regard to accepting or declining the terms without detriment.

VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON: the data subject is physically or legally incapable of giving his consent; the processing must relate to essential interests of the data subject or another person and it must in the medical context be necessary for a life saving treatment in a situation where the data subject is not able to express his intentions (e.g. an unconscious patient).

4. THE SYSTEM OF PROTECTION. ADDITIONAL SAFEGUARDS AND GUARANTEES OTHER SPECIFIC TOOLS

4.3. The 2016 CoE Recommendation on data resulting from genetic tests

E.g.: Covers the rights of persons whose personal data are processed for insurance purposes to insure against risks related to a person's health, physical integrity, age or death. Insurers need to justify the processing of health-related data and it should be proportionate to the nature and importance of the risk being considered. The processing of this kind of data is dependent on the subject's consent. Insurers should also have safeguards in place for the storage of health-related data.

4.4. Regulation (EU) No. 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and **Directive 2001/20/EC (Clinical Trials Regulation)**

5. Anonymisation and pseudonymisation

The principle of data minimization (GDPR, Convention 108)

IT security techniques / mitigate intrusions to privacy made by data processing during lawful activities

"The principles of data protection should apply to any information concerning an identified or identifiable natural person. **Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person.** To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to **anonymous information**, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purpose" (GDPRRecital 26)

6. Electronic health records

EHR

“a comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form, and providing for ready availability of these data for medical treatment and other closely related purposes”

- Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems, Point 3 (c)

Issues:

accessibility, proper storage, access by the data subject

7. DISCUSS:

1. Mr. A has taken out an insurance policy with company B, the insurer. The latter will collect some health-related information from A, such as ongoing health issues or illnesses. What should the insurer do as far as A's health-related personal data are concerned?

2. Mr. A has published on the internet the names, jobs, hobbies, telephone numbers and family circumstances of his co-workers. He also mentioned that one of them had injured his leg. He then removed all data, as some colleagues protested. Was Mr. A in breach of data protection rules? [CJEU, *The Bodil Licvist Case* C-101/01].

3. Mr. A keeps a personal diary describing incidents with friends and colleagues and health records of family members. May he be exempt from data protection rules? Why?

4. Mrs. B has recently given birth. She has had a very hard labor and there were instances when she was unconscious. While delivering, she suffered a medical emergency, due to the collapse of her cardio-respiratory system. Several medical students were present in the delivery room to observe the doctors' work. Has Mrs. A's privacy been violated? [ECtHR, *Konovalova v. Russia,* 37873/04].

5. Mr. A asked the local hospital of an EU Member States to provide photocopies of his medical file. The hospital refused, as allegedly it lacked both the resources and staff to make the copies. Did the hospital breach Mr. A's rights? [ECtHR, *K.H. and others v. Slovakia*, 32881/04].

7. DISCUSS:

6. Mrs. A was unable to prove that her health records had been accessed illegitimately by other employees of the hospital where she worked. Her claim of a violation of her right to data protection was, therefore, rejected by the domestic courts. The ECtHR noticed that the hospital's register system for health files "was such that it was not possible to retroactively clarify the use of patient records as it revealed only the five most recent consultations and that this information was deleted once the file had been returned to the archives". Moreover, the records system in place in the hospital had clearly not been in accordance with the legal requirements contained in domestic law, a fact that was not given due weight by the domestic courts. Has there been a violation of Article 8 of the ECHR? [ECtHR, *I v. Finland,* 20511/03].

7. Mrs. A complains about the submission to and use by the national courts of documents from her medical records, in the context of divorce proceedings, without her consent and without a medical expert having been appointed in that connection. In fact, it was only on a subsidiary basis that the courts had referred to the impugned medical report in support of their decisions, and it therefore appeared that they could have reached the same conclusion without it. [ECtHR, *L. L. v. France,* 7508/02].

References

https://www.echr.coe.int/Documents/Handbook_data_protection_02ENG.pdf

https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

https://rm.coe.int/16808accf8

https://www.echr.coe.int/Documents/FS_Data_ENG.pdf