WECAN SmartStart in Cancer Patient Advocacy

WECAN MASTERCLASS in Cancer Patient Advocacy

GDPR AND DATA PROTECTION: WHAT DO CANCER ADVOCATES NEED TO KNOW?

Julius Zaleskis, PhD

Founder of Dataprotection.lt

Lecturer at Vilnius University, Lithuania

info@dataprotection.lt

Content

- 1. Key elements of GDPR
- 2. How GDPR protects cancer patients?
- 3. How cancer patient organisations should comply with GDPR?
- 4. Patients related GDPR case study

1. Key elements of GDPR

- What does GDPR language mean?
- When GDPR is relevant for cancer patient organisations?
- Which parts of GDPR are old?
- Which parts of GDPR are new?
- Does GDPR already work?

What does GDPR language mean?

- Data (personal data)
- Data controller
- Data processing
- Data processor
- Data subject
- Data protection authority (DPA)
- Data protection officer (DPO)
- European Economic Area (EEA)
- General Data Protection Regulation (2016/679) (GDPR)
- Special categories of data (sensitive data)

When GDPR is relevant for cancer patient organisations?

- Collection, use and retention of data
- Healthcare service providers & cancer patient organisations as data controllers
- Patients as data subjects
- Entities established in EEA
- Entities targeting patients in EEA
- Applicability as of 25 May 2018

Which parts of GDPR are old?

- Scope of data (Art. 4(1))
- Data processing principles (Art. 5(1))
- Data processing grounds (Art. 6(1))
- Rights of data subjects (Chapter III)
- Prohibition of sensitive data processing (Art. 9(1))
- Restriction to transfer data outside EEA (Chapter V)

Which parts of GDPR are new?

- Representation of data subjects (Art. 80)
- Data protection officer (Chapter IV Section 4)
- Data protection impact assessments (Art. 35)
- Prior consultations with DPAs (Art. 36)
- Data breach notifications to DPAs (Art. 33) and data subjects (Art. 34)
- Accountability (Art. 5(2))
- Fines (4% of annual turnover / EUR 20 million) (Art. 83)
- Right to data portability (Art. 20)
- Data processor agreements (Art. 28)
- Data processing records (Art. 30)
- European Data Protection Board (Chapter VII Section 3)
- Applicability to non-EEA data controllers (Art. 3(2))
- Promotion of self-regulation (Chapter IV Section 5)

Does GDPR already work?

- February 2019: 55 955 871 EUR issued in fines (data by European Data Protection Board)
- France: 3 fines, 50 400 000 EUR
- Germany: 100 fines, 483 500 EUR
- Portugal: 1 fine, 400 000 EUR
- Denmark: 2 fines, 360 850 EUR
- Spain: 4 fines, 342 000 EUR

2. How GDPR protects cancer patients?

- Prohibition of health data
- Prohibition of genetic data
- In which exceptional cases health and genetic data can processed?
- How does a patient consent have to look like?
- What information a cancer patient has a right to know?
- What rights cancer patients enjoy?
- How can patient rights be advocated?

Prohibition of health data

- All data pertaining to the health status
- Past, current or future physical or mental health status
- Information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU
- A number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes
- Information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples
- Any information on a disease, disability, disease risk, medical history, clinical treatment
- Physiological or biomedical state of the data subject
- Source does not matter (a physician or other health professional, a hospital, a medical device or an *in vitro* diagnostic test)

Prohibition of genetic data

- Personal data relating to the inherited or acquired genetic characteristics of a natural person
- Results from the analysis of a biological sample from the natural person
- E.g.: chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or the analysis of another element enabling equivalent information to be obtained

In which exceptional cases health and genetic data can processed?

- Explicit consent of a patient
- Members of associations
- Protection of vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent
- Data manifestly made public by the data subject
- Establishment, exercise or defence of legal claims
- Reasons of substantial public interest on the basis of law
- Healthcare services
- Reasons of public interest in the area of public health
- Scientific research purposes on the basis of law

Exception of healthcare services

- Necessity:
  - to achieve the purposes for the benefit of natural persons
- Specific purposes:
  - Preventive medicine
  - Occupational medicine
  - Assessment of the working capacity of the employee
  - Medical diagnosis
  - Treatment
  - Provision or management of health or social care systems and services
- Specific legal basis:
  - EU, Member State law or a contract with a health professional
- Specific data controller:
  - Professional subject to the obligation of professional secrecy under law
- Further national conditions, including limitations, possible

Exception of public health reasons

- Necessity:
  - to achieve the purposes of society as a whole
- Specific purposes:
  - protecting against serious cross-border threats to health
  - ensuring high standards of quality and safety of health care, medicinal products or medical devices
  - other reasons of public health
- Concept of public health:
  - health status, including morbidity and disability, the determinants having an effect on that health status
  - health care needs
  - resources allocated to health care
  - the provision of, and universal access to, health care
  - health care expenditure and financing
  - the causes of mortality
- Specific legal basis
  - EU or Member State law
- No access by third parties (employers, insurance and banking companies, etc.)

How does a patient consent have to look like?

- Freely given
- Specific / granular
- Unambiguous
- Informed
- Provable
- Revocable

What information a cancer patient has a right to know?

- Identity and contact details of the data controller
- Data processing purposes
- Grounds of lawful data processing
- Data retention periods
- Rights of the data subjects
- Right to file a complaint with DPA
- Whether the data subject is obliged to provide the personal data
- The right to withdraw consent at any time
- Specific interests of the data controller or a third party
- The existence of automated decision-making, including profilig, the logic involved, envisaged consequences of such processing
- The recipients or categories of recipients of the personal data
- Transfer of data to a third country or international organisation and the ground thereof
- Contact details of the DPO

What rights cancer patients enjoy?

- Right of access
- Right to rectification
- Right to be forgotten
- Right to restriction of processing
- Right to data portability
- Right to object to data processing
- Right not be subject to automated individual decision-making, including profiling

How can patient rights be advocated?

- Complaints with DPAs
- Administrative fines
- Civil law claims for compensation
- Representation by cancer advocates:
  - not-for-profit body, organisation or association
  - properly constituted in accordance with the law
  - statutory objectives which are in the public interest
  - active in the field of the protection of data subjects' rights and freedoms
  - mandated by data subjects
  - right to lodge a complaint or receive a compensation

3. How cancer patient organisations should comply with GDPR?

- Conduct GDPR compliance audit
- Follow principles
- Establish procedures
- Consult DPO
- Revise IT security
- Educate staff

Conduct GDPR compliance audit

- Make an inventory of data based on purposes of their use
- Review internal procedures and documentation
- Check compliance of inventorised data with GDPR principles
- Identify and prioritize risks
- Draw a roadmap for compliance

Follow principles

- Specific and clear purpose of data
- As less data as possible
- Access on a need to know basis
- As less actions with data as possible
- At least one ground for processing
- Clear data deletion periods
- Transparency
- Respect for rights of individuals
- Accuracy
- Implement technical and organization security means

At least one ground for processing

- Consent of a data subject
- Contract with a data subject
- Legal obligation
- Vital interests of a data subject
- Public authority
- Legitimate interests of a patient organization
  - Where interests of a data subject are not more important
  - Need for a documented balancing test

Establish procedures

- Personal data protection policy
- Consulting DPO
- Data subject requests
- Data protection impact assessments
- Data disclosures
- Provision of information to data subjects
- Data breaches
- Data processing records
- DPA inquiries
- Data protection documentation
- IT & Data security policy

Consult DPO

- Doubts on how to comply
- Questions re internal rules and documents
- Belief that a violation occurred
- Belief that a security breach occurred
- Intention to develop data-related functionality or process
- Intention to grant access to data to someone from outside
- Doubts on whether users are informed
- Intention to use sensitive data
- Intention to monitor working tools or accounts
- Awareness of an inquiry from DPA
- Awareness of a data subject request
- Need for new documents
- Noticing of discrepancy in data processing records

Revise IT security

- Abstract principle of appropriate security of the personal data, including protection against unauthorised, unlawful processing, against accidental loss, destruction or damage (Art. 5(1)(f))
- Abstract requirement to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (Art. 32)
- No specific technical standards – this is a responsibility of a data controller
- Data security means promoted by Art. 32 of GDPR:
  - the pseudonymisation and encryption of personal data;
  - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
  - a process for regularly testing, assessing and evaluating the effectiveness of measures
  - authorisations to process data
- Need for IT assessment and IT security policy (Art. 5(2))
- ENISA's Handbook on Security of Personal Data Processing as a good practice (2018)

Educate staff

- Top management
- Legal
- Medical
- Accountancy
- Security
- Marketing
- HR
- Data analytics
- IT

4. Patients related GDPR case study

- Centro Hospitalar Barreiro Montijo was investigated by Portuguese DPA
- 9 administrative staff members had same rights of access to full medical records as doctors
- All doctors had access to full medical records notwithstanding their areas of practice
- There were 985 systems users with access to medical records while there were 296 doctors at the hospital the time of investigation
- No policy on access to patients data was adopted

Assess the situation from GDPR perspective

- Excessive access to patient records breached data confidentiality principle (Art 5(1)(f))
- Lack of access rights management breached the requirement of appropriate technical and orgnisational security means (Art. 32)
- Fine of EUR 400 000 was imposed