Pirc Musar & Lemut Strle

ODVETNIŠKA DRUŽBA

Processing of the biometric data, DNA and genomic data: development of the informational technologies or risks for rights and freedoms of the data subject

Dr. Nataša Pirc Musar. Law Firm Pirc Musar & Lemut Strle

+386 (0)1 235 50 30 \ pisarna@pirc-musar.si

Definitions – Convention 108 +

Article 6 – Special categories of data

1. The processing of:

- genetic data;
- personal data relating to offences, criminal proceedings and convictions, and related security measures;
- biometric data uniquely identifying a person;
- personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life,

shall only be allowed where appropriate safeguards are enshrined in law, complementing those of this Convention.

2. Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.

Definitions of special categories of data - GDPR

Article 9
Processing of special categories of personal data

1. 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.**

Definitions of special categories of data - GDPR

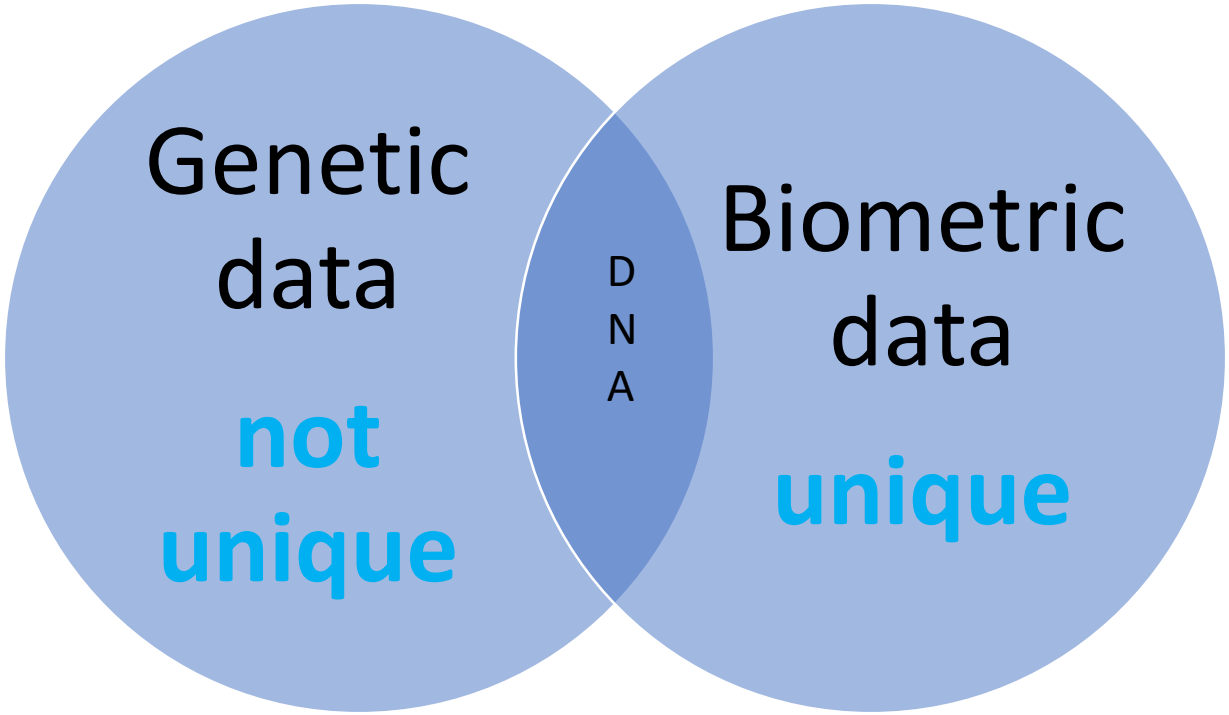
"genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

Definitions of special categories of data - GDPR

“biometric data” means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.

Private entities outside of health sector

Biometric data v genetic data



Biometric data v biometric measures

Biometric Data - **Photo (not always)**

Biometric measures - **Face recognition**

Face recognition

Smart CCTV Google

- Gorilla case (2015)

- AI
- Finger print locks
- Iris scan
- Signature

Definitions of special categories of data - GDPR

"data concerning health" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Private entities
outside of health sector

Exceptions

2. Paragraph 1 shall not apply if one of the following applies:

- Explicit Consent of the data subject
- processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State **law** or a collective agreement pursuant to Member State law providing for appropriate safeguards (**social transfers** …,
- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent (**ER**),
- processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body and that the personal data are not disclosed outside that body without the consent of the data subjects,
- processing relates to personal data which are manifestly made public by the data subject,

Exceptions

2. Paragraph 1 shall not apply if one of the following applies:

- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity,
- 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 (**criminal law, police law**),
- processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State **law** or pursuant to contract with a health professional and subject to the conditions and safeguards,
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State **law** which provides for suitable and specific measures to safeguard in particular professional secrecy (**COVID-19**),
- processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on 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.

Security measures

- Encription
  - Slovenian example (transfer of the data through electronic means - encription is obligatory)
  - Ciphered data (password)

PRIVACY BY DESIGN

- The term "**Privacy by Design**" **means** nothing more than "data protection through technology **design**." Behind this is the thought that data protection in data processing procedures is best adhered to when it is already integrated in the technology when created.
- **Privacy by design** calls for **privacy** to be taken into account throughout the whole engineering process. The concept is an example of value sensitive **design**, i.e., to take human values into account in a well-defined manner throughout the whole process.

PRIVACY BY DESIGN AND BY DEFAULT

- TECHNICAL AND ORGANISATIONAL MEASURES
- RISKS connected to processing– severity and probability taken into account
- DURING THE DETERMINATION of means of processing and implementation
- Measures: pseudonimisation, data minimization and data security Default "DATA MINIMISATION": purpose of processing; amount of data, time limit for storage, scope of data processing, availability of data → limitation of access – access rights are of significant importance – NOT ONLY HYPOTETHICALY

EU Member States

Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, **biometric data** or data concerning health.

Member States - Slovenia

Biometrics General provision Article 78

- The properties of an individual shall be determined or compared through the processing of biometric characteristics so as to identify him or confirm his identity (hereinafter: biometric measures) under the conditions provided by this Act.

Biometric measures in the public sector Article 79

- (1) Biometric measures in the public sector may only be provided for by statute if it is necessarily required for the security of people or property or to protect secret data and business secrets, and this purpose cannot be achieved by milder means.
- (2) Irrespective of the previous paragraph, biometric measures may be provided by statute where they involve compliance with obligations arising from binding international treaties or for identification of individuals crossing state borders.

Member States - Slovenia

Biometric measures in the private sector Article 80

- (1) The private sector may implement biometric measures only if they are necessarily required for the performance of activities, for the security of people or property, or to protect secret data or business secrets. Biometric measures may only be used on employees if they were informed in writing thereof in advance.
- (2) If the implementation of specific biometric measures in the private sector is not regulated by statute, a data controller intending to implement biometric measures shall prior to introducing the measures be obliged to supply the National Supervisory Body with a description of the intended measures and the reasons for the introduction thereof.

Member States - Slovenia

Biometric measures in the private sector Article 80

- (3) The National Supervisory Body shall on receipt of information from the previous paragraph be obliged within two months to decide whether the intended introduction of biometric measures complies with this Act, and in particular with the conditions from the first sentence of the first paragraph of this Article. The deadline may be extended by a maximum of one month if the introduction of such measures would affect more than 20 employees in a person in the private sector, or if the representative trade union at the employer requests to participate in the administrative procedure.
- (4) The data controller may implement biometric measures upon receipt of a decision from the previous paragraph whereby the implementation of biometric measures is permitted.
- (5) There shall be no appeal against a decision of the National Supervisory Body from the third paragraph of this Article, but an administrative dispute shall be permitted.

Member States - Slovenia

Biometric measures in connection with public sector employees Article 81

- Irrespective of the provision of Article 79 of this Act, biometric measures may be implemented in the public sector in connection with entry into a building or parts of a building and recording the presence of employees at work, and they shall be implemented with the mutatis mutandis application of the second, third and fourth paragraphs of Article 80 of this Act.

ECtHR cases

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

DNA

- **CASE OF S. AND MARPER v. THE UNITED KINGDOM,** Applications nos. 30562/04 and 30566/04) – 4.12.2008, ECtHR
- The applicant, Mr Michael Marper, was arrested on 13 March 2001 and charged with harassment of his partner. His fingerprints and DNA samples were taken. Before a pre-trial review took place, he and his partner had reconciled, and the charge was not pressed. On 11 June 2001, the Crown Prosecution Service served a notice of discontinuance on the applicant's solicitors, and on 14 June 2001 the case was formally discontinued.
- 12. Both applicants asked for their fingerprints and DNA samples to be destroyed, but in both cases the police refused. The applicants applied for judicial review of the police decisions not to destroy the fingerprints and samples

ECtHR cases

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

DNA

- **CASE OF S. AND MARPER v. THE UNITED KINGDOM**
- For the reasons set out in their submissions under Article 8, there was no reasonable or objective justification for the treatment, nor any legitimate aim or reasonable relationship of proportionality to the purported aim of crime prevention, in particular as regards the samples which played no role in crime detection or prevention. It was an entirely improper and prejudicial differentiation to retain materials of persons who should be presumed to be innocent – **VIOLATION OF ARTICLE 8.**

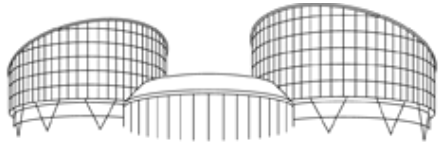
ECtHR cases

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

DNA

- **AFFAIRE AYCAGUER v. FRANCE,** Application no 8806/12, 22.7.2017
- The difference between Marper and Aycaguer case
  - (non-conviction v conviction)
  - Petty crime – police officer was hit by an umbrella – 500 EUR penalty)
  - DNA was taken (by court order)

ECtHR cases



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

- **AFFAIRE AYCAGUER v. FRANCE**
- The applicant first of all noted that, whereas the original purpose of the French national law had been to store DNA profiles of sex offenders, it now covered a wide range of offences, whatever their degree of seriousness and the extent of the public disorder which they entailed.
- the Court observes that in order to protect their population as required, the national authorities can legitimately set up databases as an effective means of helping to punish and prevent certain offences, including the most serious types of crime, such as the sex offences for which the French national law was originally created. However, such facilities cannot be implemented as part of an abusive drive to maximise the information stored in them and the length of time for which they are kept – **VIOLATION OF ARTICLE 8.**
- **DATA STORAGE – 40 years for all types of crimes**

natasa@pirc-musar.si

Pirc Musar & Lemut Strle
ODVETNIŠKA DRUŽBA
LAW FIRM

thank you