Erasmus School of Law

GDPR: Regime change in data protection law

With the support of the Erasmus+ Programme of the European Union

André den Exter

Erasmus University Rotterdam

Outline

- Context and background of European data protection law
- Terminology
- Key Principles
- Rules on lawful processing; security of processing; accountability and promoting compliance
- Supervision
- Data subjects’ rights and their enforcement
- International data transfers and flows of personal data
- Modern challenges in personal data protection

1. Context and background of European data protection law

- Right on privacy and data protection
- Legal framework
- Limitations personal data protection: Conditions under Art. 52(1) EU Charter of Fundamental Rights
- Interaction with other rights and legitimate interests

2. Terminology

- Data processing
- Profiling
- Anonymisation/pseudonymisation
- Authentication
- Controller & processor
- Consent

3. Key Principles

- The principles of lawfulness, fairness and transparency apply to all personal data processing.
- Under the GDPR, lawfulness requires either:
  - consent of the data subject;
  - necessity to enter a contract;
  - a legal obligation;
  - necessity to protect the vital interests of the data subject or of another person;
  - necessity for performing a task in the public interest;
  - necessity for the legitimate interests of the controller or a third party, if they are not overridden by the interests and rights of the data subject.
- Personal data processing should be done in a fair manner.
  - The data subject must be informed of the risk to ensure that processing does not have unforeseeable negative effects.
- Personal data processing should be done in a transparent manner.
  - Controllers must inform data subjects before processing their data, among other details, about the purpose of processing and about the identity and address of the controller.
  - Information on processing operations must be provided in clear and plain language to allow data subjects to easily understand the rules, risks, safeguards and rights involved.
  - Data subjects have the right to access their data wherever they are processed.

i. lawfulness, fairness and transparency

Lawfulness of processing: Lawful processing requires the consent of the data subject or another legitimate (Art. 5 (1) (a))

Fairness: Controllers should notify data subjects on data processing & must be able to demonstrate the compliance of processing operations with the GDPR

e.g., *K.H. and Others v. Slovakia:* access to medical data

Transparency: personal data processing “in a transparent manner”

e.g., *Haralambie v. Romania:* shortcomings archive system does not justify a 5- years delay in granting request access applicant’s files

Transparency on risks/rules/safeguards and rights regarding the processing of their personal data

ii. The principle of purpose limitation

- Defined purpose before processing is started

- No further processing of data in a way that is incompatible with the original purpose, though the General Data Protection Regulation foresees

  Exceptions: for archiving purposes in the public interest, scientific research and statistical purposes

- In essence, processing of personal data must be done for a specific well-defined purpose and only for additional, specified, purposes that are compatible with the original one.

  E.g., passengers booking info used for immigration purposes?

iii. The data minimisation principle

- Procesing limited to what is necessary to fulfil a legitimate purpose
- The processing of personal data should only take place when the purpose of the processing cannot be reasonably fulfilled by other means
- Data processing may not disproportionately interfere with the interests, rights and freedoms at stake

iv. The data accuracy principle

The principle of data accuracy must be implemented by the controller in all processing operations

Inaccurate data must be erased or rectified without delay

Data may need to be checked regularly and kept up to date to secure accuracy

But updating medical record prohibited!

Otherwise: updating can be absolutely necessary!

v. The storage limitation principle

Personal data must be deleted or anonymised as soon as they are no longer needed for the purposes for which they were collected (Art. 5(1) (e))

"time limits should be established by the controller for erasure or for a periodic review"

E.g., indefinite retention of the fingerprints, cell samples and DNA profiles applicants was disproportionate and unnecessary as criminal proceedings had been terminated (*Marper v UK*)

Note: time limitation for *identifiable* data

vi. The data security principle

- Security and confidentiality of personal data is key to adverse effects for the data subject
- Security measures can be of a technical and/or organisational nature
- Pseudonymisation is a process that can protect personal data
- The appropriateness of security measures must be determined on a case-by-case basis and reviewed regularly

E.g. “Charles Spencer, born 3 April 1967, is the father of a family of four childr
boys and two girls” pseudonymised by: CS, 1967 is the father of a famil ”

vii. The accountability principle

- Controllers and processors to required to promote and safeguard data protection in processing activities

- Controllers are responsible for compliance of their processing operations with data protection law

- Controllers must be able to demonstrate compliance with data protection provisions to data subjects, the general public and supervisory authorities at any time, including:

  - keeping a record of processing operations

  - appointing a Data Protection Officer

  - performing data protection impact assessments for certain types of processing

  - ensuring data protection by design and by default

4. Rules on lawful processing: Consent is King!

- **Consent**: Cornerstone for the processing of personal data

  "freely given, informed, specific and unambigious" (Art. 6 GDPR & Art. 8 EU Charter)

- The right to withdraw consent at any time

i. Health Data: Specific regime (art. 9(1))

"all data pertaining to the health status of a data subject which reveal information relating to the past/current/future physical/mental health status of the data subject", as well as genetic data

- Prohibited, *unless* it is authorised under Art. 9(2):
  - explicit consent
  - preventative or occupational health purposes, medical treatment, or management of healthcare services (h)
  - public health (i)
  - research and statistical purposes (j) & art. 89

- Additional conditions under national law (genetic, health-related data)

- Clinical trials and DP implications & Electronic health records

5. Rules on security of processing

- to implement appropriate technical and organisational measures to prevent any unauthorised interference with data processing operations (Art. 32)

Measures may include :

- Pseudonymising and encrypting personal data
- Anonymisation
- Confidentiality clauses

Elements of data security: *to ensure a level of security appropriate to the risk*

But which level?

Data security is not just achieved by having the right equipment – hardware and software – in place. It also requires appropriate internal organisational rules.

Cyber security: Hacks and breaches

'Professional' hack on Norwegian health authority compromises data of three million patients

Local security centre blames breach on 'advanced' hackers

HACKERS HAVE BREACHED the systems of Norway's Health South East RHF, with nearly three million patients' data potentially compromised as a result.

Hospital staff given access to patient records for research without consent - report

Major investigation by Data Protection Commissioner examines privacy practices at 20 hospitals

NHS hack: Cyber attack takes 16 hospitals offline as patients are turned away

Hospitals in London, northwest England and elsewhere have all been knocked offline

ii. Personal data breach notifications

Data breaches are still a common phenomenon

Consequences

Notification requirement: detailed regime regulating the timing and content (Arts. 33-34)

- Within 72 hours notification breaches supervisory body
- minimum information
- Informing data subject (high risks breach)

6. Rules on accountability and promoting compliance

To guarantee the enforcement of the data protection rules in Europe

Instruments:

- the appointment of data protection officers (DPO, Art. 37(1))
- impact assessment before starting (high risk) processing activities (Art. 35)
- prior consultation supervisory authority
- codes of conduct for controllers and processors

7. Independent supervision

- Criteria of ‘complete independence’ (Art. 69)
- Competence and powers
- Cooperation
- European Data Protection Board

8. Data subjects' rights and their enforcement

- Right to be informed (Arts. 12-14)
- Right to rectification (Art. 16)
- Right to erasure ('the right to be forgotten') (Art. 17)
- Right to restriction of processing (Art. 18)
- Right to data portability (Art. 20)
- Right to object (Art. 21(1)(2))

i. Remedies, liability, penalties and compensation

- Right to lodge a complaint with a supervisory authority (Art. 57(2))
- Right to an effective judicial remedy
- Sanctions (Art. 83)

9. International data transfers and flows of personal data

- Free flow of data within the European Union
- Transfer to third-countries: ‘appropriate’ safeguards (Art. 46)

10. Modern challenges in personal data protection

New technologies: Big data, algorithms and artificial intelligence

"*an open and informed discussion on digital ethics, which allows the EU to realise the benefits of technology for society and the economy and at the same time reinforces the rights and freedoms of individuals, particularly their rights to privacy and data protection*"

Health, data protection and privacy implications: advantages and risks

Summary

- Core principles broadly the same, but tighter controls
- Greater accountability and shift in burden of proof
- Increased records and compliance burden

References

- EU FRA, *Handbook on European data protection law,* Luxembourg 2018 edition

- What does the GDPR mean for the medical community? *LANCET,* 391 (1027), 1249-1250, MARCH 31, 2018

- J. Rumbold et al, The Effect of the General Data Protection Regulation on Medical Research, *J Med Internet Res*. 2017 Feb; 19(2): e47

Discussion: Case studies

Estonia, the Genetic Biobank: Opening Pandora's Box?

- **Free genetic testing** to 100,000 citizens. The participants will donate blood samples to the Estonian biobank, which will conduct a genome-wide genotyping and alert those among them who are likely to suffer from conditions like cardiovascular disease, type 2 diabetes, and breast cancer

- **Main goals**: to help the Estonian healthcare system identify who are at risk for certain diseases; to reduce healthcare costs and improve citizens' quality of life

- The Estonian biobank has created already a reliable disease prediction algorithm
- Database will not only be used to prevent diseases, but also to improve current treatments. At present, the Estonian biobank can give accurate feedback for 28 medications, many of which are widely prescribed.
- After adding the 100,000 samples in this round, the Estonian biobank will have the genetic profile of about 10 percent of Estonians

Combining data sources and re-use of Health Data to support Public Health Research?

Research in public health is transitioning from siloed systems to more accessible and re-usable data resources. Following the example of the Nordic countries, several European countries aim at facilitating the **re-use** of their health administrative databases for research purposes. However, the ecosystem is still a complex patchwork

Case study Telemedicine and Data transmission

- Patient X, affiliated to the Country A social security system, suffers from chronic gall bladder problems. The treating healthcare provider in Country A puts the patient in touch with a surgical centre of excellence specialising in digestive systems in Country B. A well-renowned healthcare professional based in Country B would be able to operate on Patient X through telesurgery. A series of medical tests and important health-related patient data are requested by the Country B based operating doctor.
- The key sensitive medical information is therefore to be transferred electronically across borders between Country A and Country B.