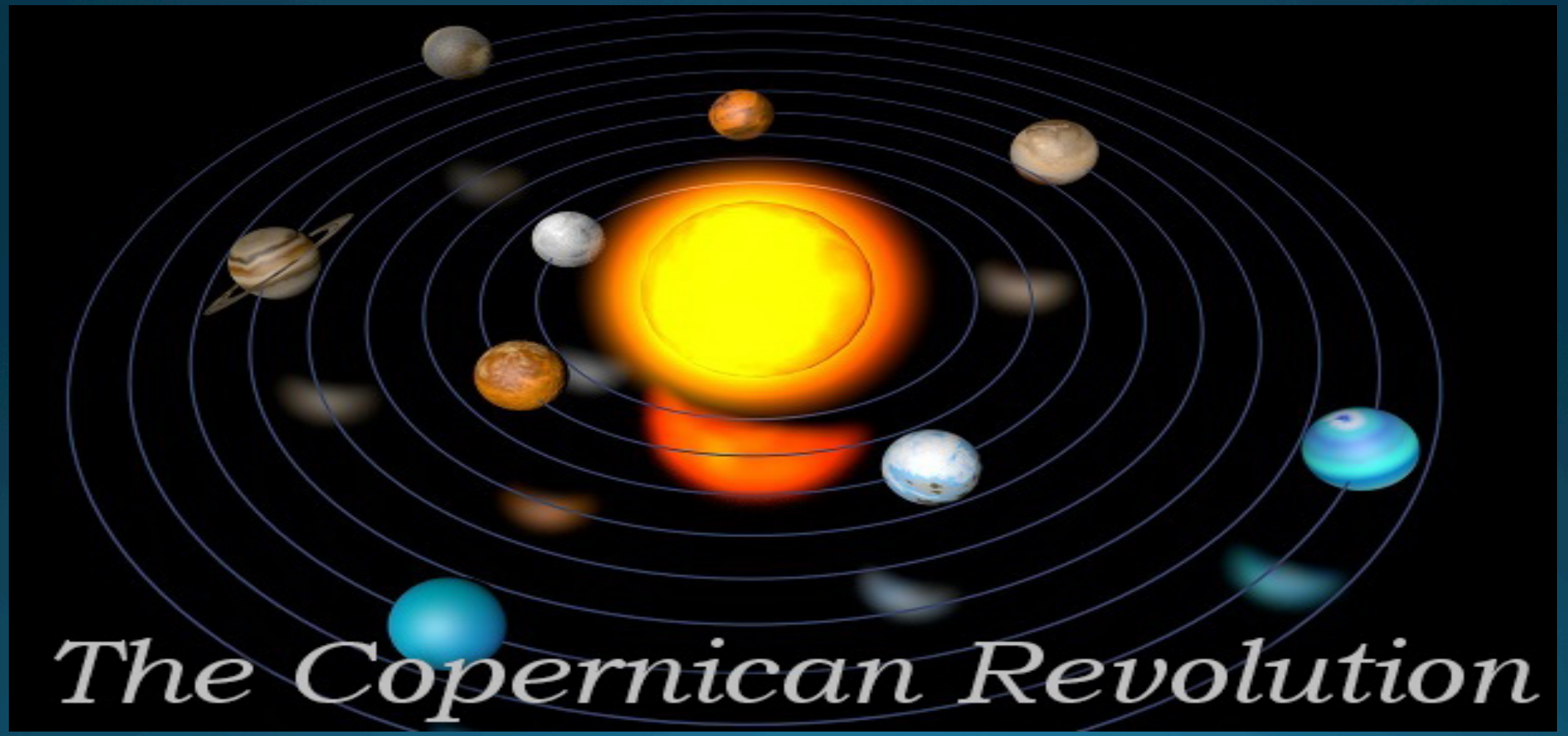
A Game Changer for Research? GDPR and Health Data

Dr Nora Ni Loideain
Director and Lecturer in Law
Information Law and Policy Centre
IALS, University of London

Outline

- An overview of the *development and key reforms* of the EU General Data Protection Regulation (679/2016) (*GDPR*).
- Examine the scope, lawful basis, conditions, and safeguards governing provisions concerning research and health data.
- Address the implications and challenges of these requirements for research and health data.

GDPR – a ‘Game Changer’?



GDPR – Data Protection for the 21st Century

- Information Commissioner (UK's Data Protection Authority): 'GDPR brings data protection into the 21st century'.

- Draft proposals *in 2012 – late 2015*, GDPR developed by trilogue between EU Institutions.

- Enacted May 2016, implementation required by *25 May 2018*, Evaluation in 2023.

GDPR – Evolution and Revolution

- Main concepts (personal data, processing, consent), principles, aims, framework remain.

- Key principles relevant to research remain

- Fair and Lawful (and transparent) processing
- Purpose limitation
- *Data minimisation*
- Accuracy and quality
- Storage limitation
- Integrity, *security*, and confidentiality (data access, encryption).

GDPR – Evolution and Revolution

- Develops new concepts, sanctions, and provides new rights: principle of ‘data protection by design’.

- But also *clarifies and strengthens* requirements *governing existing rights* and obligations, e.g. transparency surrounding consent and privacy notices.

- Co-regulatory approach: a *major shift in accountability* from data protection authorities to *data controllers* and *data processors (DPIA, POPI Audit)*

EU Data Protection Law – need for reform

EU Commission, 2003 *Report on Directive 95/46 Implementation*; 2012 *Safeguarding Privacy Report:*

1. *Nebulous* provisions with varying levels of *guidance*

2. Divergences in implementation – *lack of harmonisation*

3. *Under-resourced*/lack of independent data protection authorities (DPAs)

EU Data Protection Law – need for reform

- Need for privacy-enhancing technologies (PETs)
- '*Patchy compliance*' by data controllers
- Complaints regarding divergences in interpretation and supervision by data protection authorities (e.g. POPI Regulator), esp. from multinational companies
- Low level of knowledge among data subjects

GDPR – a ‘Game Changer’?

- *Reasonable or unworkable*? Will the increased scope and responsibility on data controllers work in practice?

- Do the exemptions and restrictions provide for *an adequate balance* with other fundamental rights and legitimate interests, e.g. medical and health research

- *28 legal systems* to one - total harmonisation under GDPR?

GDPR – A Game Changer

GDPR – Expands Global Reach of EU Law

- GDPR (art.3) expands *territorial application* of EU Data Protection Law – implications for research is unclear.

- Data controllers/processors *not established in the EU* will be subject to the GPDR if …

- They process the personal data of *individuals within the EU* for purposes related to offering them goods/services or *by monitoring their behaviour*.

GDPR – a Regulation, not a Directive

- Unlike EU directives, EU regulations have *general application and are directly applicable* (allows for fewer differences in implementation by EU Member States).

- Immediately part of national law; no need to adopt separate national legislation; has legal effect independent of national law; and overrides contrary national laws.

- Should lead to *a greater degree of harmonization and less divergence* between Member State laws = greater legal certainty and better for compliance.

GDPR – a ‘Game Changer’

GDPR – a ‘Game Changer’

- European Commission in 2012 stated GDPR would both ‘*enhance*’ rights of data subjects and *cut ‘red tape’* for data controllers …

- Reforms under GDPR (new rights, obligations, *sanctions*) viewed by some as bold, ambitious, and *optimistic.*

- Provides data protection authorities across EU *with equal enforcement powers* and sanctions – fines of 4% or 2% of Total Worldwide Annual Turnover (up to 20, 000,000 euro or more) (ICO upper fine limit: £500, 000).

GDPR –
New Administrative Fines are coming …

GDPR, Health, and Research Purposes ...

A Game Changer?

Broad scope for research purposes

- Four specific research purposes, all *'subject to appropriate safeguards'.*
- *Scientific research*; historical research; archiving in the public interest and statistical purposes ('the research purposes').
- Application of term is intended to be *wide*, also covers social science research.

‘Scientific Research Purposes’

- GDPR, recital 159:

‘[T]he processing of personal data for scientific research purposes should be interpreted *in a broad manner*, including for example,

technological development and demonstration, *fundamental research*, *applied research* and *privately funded research*’.

Scope of personal data

- GDPR essentially carries forward existing *very broad concept* under EU Data Protection Directive (1995).

- *Any data* that makes an individual *'identifiable'*, therefore - GDPR does not apply to processing of *anonymous* information for research purposes.

- GDPR, recital 26: falls within the scope of personal data if a *natural person* can be *singled out* – any 'identifier', e.g. name, ID, genetic factor, address (offline/online).

Stricter requirements for ‘special categories’

- Special category data replaces concept of ‘*sensitive’ personal data.*
- GDPR, art.9: Processing of this type of data is prohibited unless specific conditions apply – *a qualified prohibition*.
- Scope *includes* personal data that reveals ‘racial/ethnic origin’, political opinions, religious beliefs, genetic data, *data concerning health*.

Data concerning health

- Very broad scope

- GDPR, art.4(15): ‘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’.

- GDPR, recital 35 provides more detail and examples.

Data concerning health

Data concerning health

- '*Should include* … all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status'.

- Includes a number … to uniquely identify the natural person for health purposes (e.g. national health ID, health insurance policy number).

- Information derived 'from testing/examination of a body part or bodily substance, including from genetic data and biological samples; any information on, *for example*, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject … '

Safeguarding Requirements for Research Purposes

- GDPR, art.89: safeguards must be in place that protect *rights* and freedoms of the data subjects:
- Right of access (e.g. privacy notices) (GDPR, art.15)
- Right of rectification (principles of accuracy & integrity)(GDPR, art.16)
- Right to restriction of processing (GDPR, art. 18)
- Right to object (unless research is needed for public interest task)(GDPR, art.21)

Safeguarding Requirements for Research Purposes

- '*Technical and organisational* measures' must be place to ensure compliance with principle of *data minimisation*, e.g. pseudonymisation.

- Hence, researchers should *record/log* safeguards measures taken (eg time limits for data storage/deletion);

- Use *identifiers* only when shown to be necessary.

Technical measures - anonymous data?

Safeguarding Requirements for Research Purposes

- *Is anonymisation* - rendering information entirely unidentifiable to a living individual - *possible* in the research environment?

- If so, that information is *not personal data* and therefore falls outside the data protection legal framework …

- However, difficult to ensure in practice as research tends to require some form of identifier *to link records or distinguish different datasets*.

Alternatively - Pseudonymisation?

- *No - still falls* within data protection legal regime – treated as one of the safeguarding technical measures to adopt.

- GDPR, recital 26: processing personal data in such a manner that said data can no longer be attributed to a specific data subject *without the use of additional information* – identifiers should be stored separately, secured, with limited access.

- E.g. using cryptography, key code for non-aggregated data: ‘the individual coded *X1234* drinks a glass of wine more than 3 times a week'.

Looking forward and implementation

- GDPR, art.89: Member States are permitted to have different requirements for processing health data *'in so far as such rights are likely to render impossible or seriously impair'* the relevant research.

- Hence, researchers from outside the EU – third countries (e.g. South Africa, U.S., UK …) undertaking research on health-related data …

- Need to pay special attention to derogations adopted by specific Member States depending on nationality of EU individuals' health data, e.g. Ireland, Germany, France.

European Data Protection Board – Further guidelines and requirements

- GDPR, art.68 EDPB - a legal entity to *replace advisory Art.29 Working Party*, will be hosted by an expanded and reinforced EDPS secretariat (GDPR, art.75).

- *Secretariat of EDPB* (Art.29 WP) to be *independent* from Commission: Dir. 95/46, art. 29(5).

- EDPS will have a *crucial role* at EU-level in providing specific GDPR guidance for data protection compliance in the research sphere.

Summary: A Game Changer

- Stricter requirements for researchers in terms of data management and security.
- Non-EU countries will have to scrutinize the individual GDPR laws of relevant EU Member States on restrictions and exemptions.
- Greater responsibility for data processors (researchers processing data *on behalf* of the lead research decision-making centre).

Conclusion

- Questions?

- Thank you.

Website: http://ials.sas.ac.uk/about/about-us/people/nóra-ni-loideain
Twitter: @noraniloideain
ILPC Twitter: @infolawcentre