The University Of Sheffield.

The General Data Protection Regulation (GDPR): using personal data for scientific research

Digital healthcare: cutting edge innovation

8th February 2018

Vicky Chico

NHS Health Research Authority

 © The University of Sheffield

Focus

Key provisions for research

- Principles
- Lawful bases for processing
- Consent
- New rights if consent is the lawful basis

Not covering organisational compliance or the Data Protection Bill

 © The University of Sheffield

Scope and definitions

- GDPR covers all processing of personal data
- Definition of personal data
- Does not apply to anonymous information
- Restrictive in many areas of data processing more enabling in the context of scientific research

 © The University of Sheffield

Preparing for the General Data Protection Regulation (GDPR) 12 steps to take now

1 Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2 Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3 Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4 Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.

5 Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6 Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7 Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8 Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9 Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10 Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11 Data Protection Officers

You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12 International

If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

ico. Information Commissioner's Office

ico.org.uk

V2.0 201705

The University Of Sheffield.

Article 5

Principles relating to processing personal data

(a) Lawfulness, fairness and transparency
(b) Purpose limitation
(c) Data minimisation
(d) Accuracy
(e) Storage limitation
(f) Integrity and confidentiality
(g) Accountability

NHS Health Research Authority

 © The University of Sheffield

Article 5 Principles

Research exemptions to the principles

(b) collected for specified and legitimate purposes and not further processed in a manner which is incompatible with those purposes (purpose limitation)

(b) further processing for **scientific purposes** shall not be considered to be incompatible with the initial purpose (purpose limitation)

© The University of Sheffield

The University Of Sheffield.

Article 5 Principles

Research exemptions to the principles

(e) kept in a form which permits identification for no longer than is necessary for the purposes (storage limitation)

(e) personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, **scientific** or historical **research** purposes or statistical purpose (storage limitation)

NHS Health Research Authority

 © The University of Sheffield

Article 6
Lawfulness of processing

Six bases for lawful processing

- Consent
- Contract
- Vital interests
- Public interest or official authority
- Legitimate interests

Processing of personal data for research purposes by a public authority such as a UK university or NHS organisation:

- necessary for the performance of a task carried out in the public interest or in the exercise of official authority (Article 6(1)(e))

© The University of Sheffield

The University Of Sheffield.

Article 9

Processing special categories of personal data

- Racial or ethic origin
- Political opinions, religious or philosophical beliefs
- Trade union membership
- **Genetic and biometric data**
- **Health data**
- Sex life and sexual orientation

Processing generally prohibited unless one of ten conditions applies

NHS Health Research Authority

 © The University of Sheffield

The University Of Sheffield.

Article 9

Processing special categories of personal data

Processing special categories of personal data for research:

a. The data subject has given **explicit consent** to the processing of those personal data for **one or more specified purposes**

j. Processing is necessary for archiving purposes in the public interest, **scientific** or historical **research purposes** or statistical purposes

NHS Health Research Authority

 © The University of Sheffield

The University Of Sheffield.

Article 9

Processing special categories of personal data

(j) Processing necessary for **scientific research purposes**

Must be in accordance with the safeguards in Article 89(1)

Article 89(2) derogations where **rights** are likely to render impossible or seriously impair the achievement of the specific purposes

Data Protection Bill provides for derogations from some GDPR rights

NHS Health Research Authority

 © The University of Sheffield

The University Of Sheffield.

Article 89 (1)

Safeguards relating to processing for scientific research purposes

Processing for scientific research purposes shall be subject to appropriate safeguards in accordance with this regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to respect the principle of **data minimisation**. Those measures may include **pseudonymisation** provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which **does not permit or no longer permits the identification** of data subjects, those purposes shall be fulfilled in that manner

NHS Health Research Authority

 © The University of Sheffield

The University Of Sheffield.

Articles 6 and 9

The lawfulness of processing

Data controllers must establish and publish their lawful basis and any condition for processing special categories of personal data

NHS Health Research Authority

 © The University of Sheffield

The University Of Sheffield.

Article 4

Definition of consent

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her

The GDPR does not give a definition of 'explicit consent' required under Article 9

NHS Health Research Authority

 © The University of Sheffield

The University Of Sheffield.

Article 7
Conditions for consent

Where processing is based on consent the controller must demonstrate the data subject has consented

If consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from other matters

Data subject shall have the right to withdraw consent at any time. It must be as easy to withdraw consent as giving it

NHS Health Research Authority

 © The University of Sheffield

The University Of Sheffield.

Consent continued

Consent is one way to comply with the GDPR. It is not the only way

In some contexts GDPR compliant consent may be difficult

Caution in the case of an imbalance of power

Consent is not preferred over other legal bases. There are practical implications where an organisation relies on consent

NHS Health Research Authority

 © The University of Sheffield

Consent continued

GDPR requirements do not affect the common law duty of confidence. Organisations do not need to change their consent practices to comply with the GDPR in order to maintain confidence

However consent obtained or assumed for reasons of confidentiality may not comply with the GDPR

It is only if the organisation relies on consent as the lawful basis for processing under the GDPR that the consent needs to be GDPR compliant

 © The University of Sheffield

The University Of Sheffield.

Consent continued

What does this mean for the concept of broad consent under the GDPR?

'It is often not possible to fully identify the purpose of personal data processing for **scientific research purposes** at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of **scientific research** when in keeping with recognised ethical standards for **scientific research**. Data subjects should have to opportunity to give their consent only to certain areas of research'

Recital 33

NHS Health Research Authority

 © The University of Sheffield

Articles 15-22
Rights of the data subject

In addition to setting a high standard, where processing is based on consent the data subject enjoys a number of rights linked to consent:

- The right to withdraw consent
- The right to data portability

Alternatives to consent

© The University of Sheffield

Articles 15-22

Rights of the data subject

Derogations under Article 89(2) and the UK Data Protection Bill

Article 15 – Right of access
Article 16 – Right to rectification
Article 18 – Right to restriction of processing
Article 21 – Right to object

Further, there is a specific provision in Article 17 – the right to erasure that limits the application of that right where processing is necessary for achieving **scientific research purposes**

 © The University of Sheffield

The University Of Sheffield.

Conclusion

- Centred around key principles of lawfulness, fairness transparency and accountability
- Significant exemptions for scientific research
- Consent may be difficult to achieve and may not be the most appropriate legal basis for processing of personal data for achieving scientific research purposes

NHS Health Research Authority

 © The University of Sheffield