phg foundation
making science work for health

How does the GDPR apply to the sharing of genetic and genomic data?

Colin Mitchell
Senior Policy Analyst

UNIVERSITY OF CAMBRIDGE

Research: The GDPR & Genomic Data

phg foundation making science work for health

Research questions:

- To what extent do genetic/genomic data used for healthcare and medical research count as personal data under the GDPR?
- To the extent that genomic data count as personal data, what impact might this have on the delivery of health and social care in the short to medium term (i.e. within the next 5 years)?
- How can potential deleterious impacts be mitigated or reduced?

ico. Information Commissioner's Office — Grant Recipient

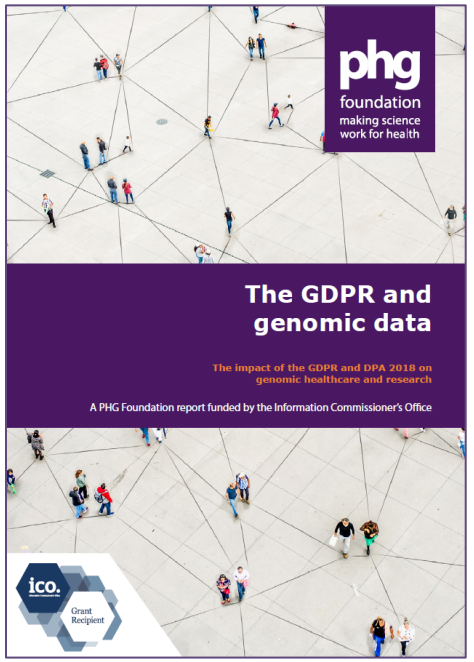
Methods:

- Review and analysis of literature, case law and legislation
- Key stakeholder interviews
- Multidisciplinary workshop (30+ delegates)

Outputs:

- **Project Report**, Executive Summary & Policy Briefing

https://www.phgfoundation.org/report/the-gdpr-and-genomic-data



Outline: how the GDPR applies

phg foundation
making science work for health

1. The EU GDPR
2. Where it applies
3. Rules for transfer of genomic data outside the EU/EEA
4. Ways ahead for the genomics community

EU General Data Protection Regulation

phg foundation
making science work for health

Regulation (EU) 2016/679

- Into force since 25th May 2018
- Applies to all sectors and forms of 'processing'
- Based on a fundamental right to data protection
- New governance requirements, e.g. potential fines up to 4% global annual turnover
- Enhanced rights and obligations (e.g. right to be forgotten)

phg foundation
making science work for health

How does the GDPR apply to international genomic data sharing?

1. Territorial Scope

The GDPR's scope isn't limited to Europe- it will apply if data are processed outside Europe:

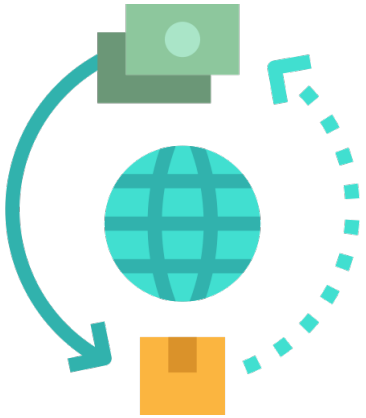
- Either because there is a sufficient link with the activities of an institution established in the EU/EEA, or;
- Where there is offering of goods or services, or monitoring of the behaviour of data subjects who are in the EU/EEA

Implications:

- Could capture genomic research conducted outside Europe if, for example, the research is directed or controlled by an institution within Europe.
- Also is possible this could capture the monitoring of the clinical data of individuals in Europe by a research biobank based elsewhere.

2. Transfers outside the EU/EEA

For anything but exceptional transfers, this is only possible within a hierarchy of specific legal mechanisms (Chapter V)



***Schrems II* decision**

- EU-US Privacy Shield declared invalid
- For most mechanisms data controllers must evaluate the legal framework of non-EU countries to ensure they offer adequate equivalent protection for personal data!

Implications:

Difficult to see how these high standards can be met in some contexts.

3. Disagreement on GDPR requirements?

Many other aspects of compliance with the GDPR must be agreed by joint controllers and collaborators, e.g. the legal basis for processing. However:

- High GDPR standards, for example for reliance on consent as a legal basis, can mean this is not straightforward
- Considerable scope for national variation and differences in interpretation mean it is challenging to reach agreement between parties

Implications:

Significant time and resources required to reach agreement between collaborators on legal bases under GDPR, safeguards and procedures for enabling relevant data subject rights (amongst others!).

4. Broad scope of 'personal data'

Can this be avoided by anonymising data so that they are no longer personal data governed by the GDPR?

- The GDPR requires a broad contextual assessment of risk of identification and this can be hard to achieve in the case of genomic data
- e.g. the status of data that have been pseudonymised (or key coded data) is not straightforward: even if data are no longer connected with the key, they may be considered 'personal data' by some authorities

Implications:

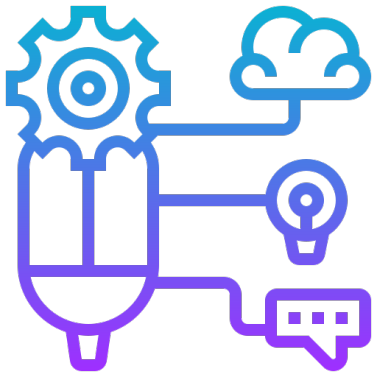
It may be difficult obtaining agreement from all parties in a genomic data sharing collaboration that data are no longer 'personal data'

Ways ahead?

phg foundation
making science work for health

Technical approaches:

- Bringing analysis to the data rather than sharing personal data e.g. cryptographic techniques such as homomorphic encryption to facilitate data analysis without disclosing personal data



Developing codes of conduct (Art 40) or certification schemes (Art 42):

- Crystalise best practice and consensus about key safeguards and legal interpretations in the genomic context
- Potential to be used as legal mechanism for international data transfers (this is untested)

Advocacy for appropriate standards for genomic data sharing

- In EDPB guidance
- Even calls for amendments by the EU legislature

Thank you!

GDPR and genomic data report available here:
https://www.phgfoundation.org/report/the-gdpr-and-genomic-data

Contacts:
Colin.Mitchell@phgfoundation.org
Alison.Hall@phgfoundation.org


UNIVERSITY OF
CAMBRIDGE


phgfoundation
making science work for health