UNIVERSITY OF CAMBRIDGE

PHG FOUNDATION
making science work for health

The GDPR, UK GDPR and international transfers of personal data

The EU General Data Protection Regulation (GDPR) and the United Kingdom's version of the same regulation (the 'UK GDPR') set out rules that govern transfers of personal data to 'third countries' or international organisations. This short note provides an overview of the key provisions and some of the challenges they present for international genomic and health data sharing.[1]

WYNG FOUNDATION

Personal data are defined in the GDPR as:

'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Art 4(1))'

The EU GDPR and the 'UK GDPR'

Although the UK left the European Union in January 2020, laws based on EU regulations were carried over into the UK legal framework. This includes the GDPR which is now incorporated, with some essential modifications, as the 'UK GDPR'.[2] Crucially, the UK has also secured an 'adequacy' agreement with the EU which allows free flow of data between the EU/EEA and the UK to continue until 2025. Therefore, at present, the rules governing transfers of personal data between the UK and the rest of the world are virtually identical to the EU law. For this reason, this note mainly refers to the EU GDPR.

Chapter V general rule

Chapter V of the GDPR governs transfers of personal data to a 'third country' or international organisation. Third countries are those outside the EU/EEA (which now also includes the UK). The general rule (Article 44), which has been reaffirmed by the Court of Justice of the European Union (CJEU) in a series of cases on EU-US data transfers involving Facebook (Schrems I[3] & Schrems II[4]), is that transfers should only take place where a controller is satisfied that there is an adequate or 'essentially equivalent' level of protection in the receiving jurisdiction.

The CJEU has emphasised that this is a very high standard which includes an assessment of whether the fundamental rights and freedoms of data subjects are protected in accordance with the Charter of Fundamental Rights of the European Union. This causes particular challenges for transfers to third countries with potential state surveillance of data (as is the case in the United States). The CJEU has ruled that such jurisdictions cannot provide an essentially equivalent level of protection without (at least) some key safeguards for EU/EEA data subjects:

- Processing should be based on clear, precise and accessible rules
- Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated
- An independent oversight mechanism should exist
- Effective remedies need to be available to the (EU) individual[5]

Apart from transfers based on an adequacy decision (discussed below), it is the responsibility of the data exporter in the EU to assess the level of protection provided in the circumstances of the transfer at hand, presenting a significant challenge for data exporters.

Chapter V provides three main mechanisms that can be used to transfer personal data to third countries or international organisations: adequacy decisions (Art 45), appropriate safeguards (Art 46) and derogations for specific situations (Art 49).

Adequacy (Art 45)

The simplest method is a data transfer on the basis that the EU has recognised the recipient jurisdiction as offering an adequate level of data protection. Nothing more is necessary to legitimise the transfer in this case and the only risk is that (as seen in the Schrems cases) an adequacy decision can be contested in the CJEU. The drawback of this mechanism is that only a handful of jurisdictions have been recognised as adequate by the EU: Excluding the UK, the European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan (private sector), Jersey, New Zealand, Republic of Korea, Switzerland and Uruguay as providing adequate protection. For other jurisdictions, an alternative mechanism will be required.

Appropriate safeguards (Art 46)

In the absence of an adequacy decision, the next potential mechanism is use of 'appropriate safeguards' to protect the data. These may include:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules in accordance with Article 47;
- standard data protection clauses;
- an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments; or
- an approved certification mechanism with binding and enforceable commitments.

Although there are a range of options, researchers and academics have identified challenges regarding their suitability in the research and genomic context[6] (see table below).

Safeguard	Challenges in genomic/research context
A legally binding and enforceable instrument between public authorities or bodies	Must be adopted in full. This gives rise to potential statutory conflicts with third country organisations who cannot agree to clauses such as redress clauses e.g. the US NIH.
Standard data protection contract clauses adopted/approved by the European Commission/national authorities	
An approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or	Untested for international transfers. Lengthy process to agree codes or certification and untested in terms of what may be sufficient to serve as an appropriate safeguard for international transfers.
An approved certification mechanism pursuant to Article 42	
Binding corporate rules in accordance with Article 47	Limited applicability as only available for transfers within multinational entities

The CJEU's judgment in Schrems II has also led to a fundamental difficulty with all these safeguards, which is that they may not be sufficient in themselves to ensure an essentially equivalent level of protection in the circumstances of the transfer.

'Supplementary measures' may be needed to achieve an adequate level of data protection. The European Data Protection Board (EDPB) has recommended some supplementary measures that could be considered on a case-by-case basis.[7] These include technical measures, such as pseudonymisation, additional contractual measures, for example an obligation to provide an assessment of the legal framework in the importing jurisdiction, and, organisational measures, such as the adoption of ISO standards or other best practice policies. Unfortunately, although many of these measures are often included in genomic and scientific data sharing agreements as a matter of course, the way they are interpreted by the EDPB does not necessarily match what is feasible in health research. For example, the standard for pseudonymisation in EDPB guidance exceeds how it is otherwise defined in the GDPR and generally applied to health data.[8]

In addition, as the EDPB acknowledges, supplementary measures may not be sufficient in all circumstances and the risk remains with the exporting controller to ensure adequate protection.

Derogations (Article 49)

If it is not possible to use safeguards to legitimise an international transfer, then Article 49 GDPR sets out some limited derogations. Article 49 derogations offer a set of legal mechanisms to lawfully transfer personal data to third countries or international organisations. However, the EDPB has emphasised that these should only be used as an exception to the requirement for either adequacy or appropriate safeguards, and as a consequence, that their applicability should be interpreted restrictively.[9] The derogations include:

a. Where the data subject has explicitly consented to the transfer

b. Where the transfer is necessary for the performance of a contract between the data subject and controller

c. Where the transfer is necessary for the conclusion or performance of a contract in the interest of the data subject

d. Where the transfer is necessary for 'important reasons of public interest'

e. Where the transfer is 'necessary for the establishment, exercise or defence of a legal claim'

f. Where the transfer is necessary in order to protect the vital interests of the data subject

g. Where the transfer is made from a public register

In addition to these explicitly stated derogations, there is also a final 8th derogation listed in the second paragraph of Article 49(1) invoking 'compelling legitimate interests'.

While these derogations may be used in exceptional circumstances (and for example have been used in a limited way during the COVID-19 pandemic), they are not suitable for long-term and routine genomic and health data transfers.[10]

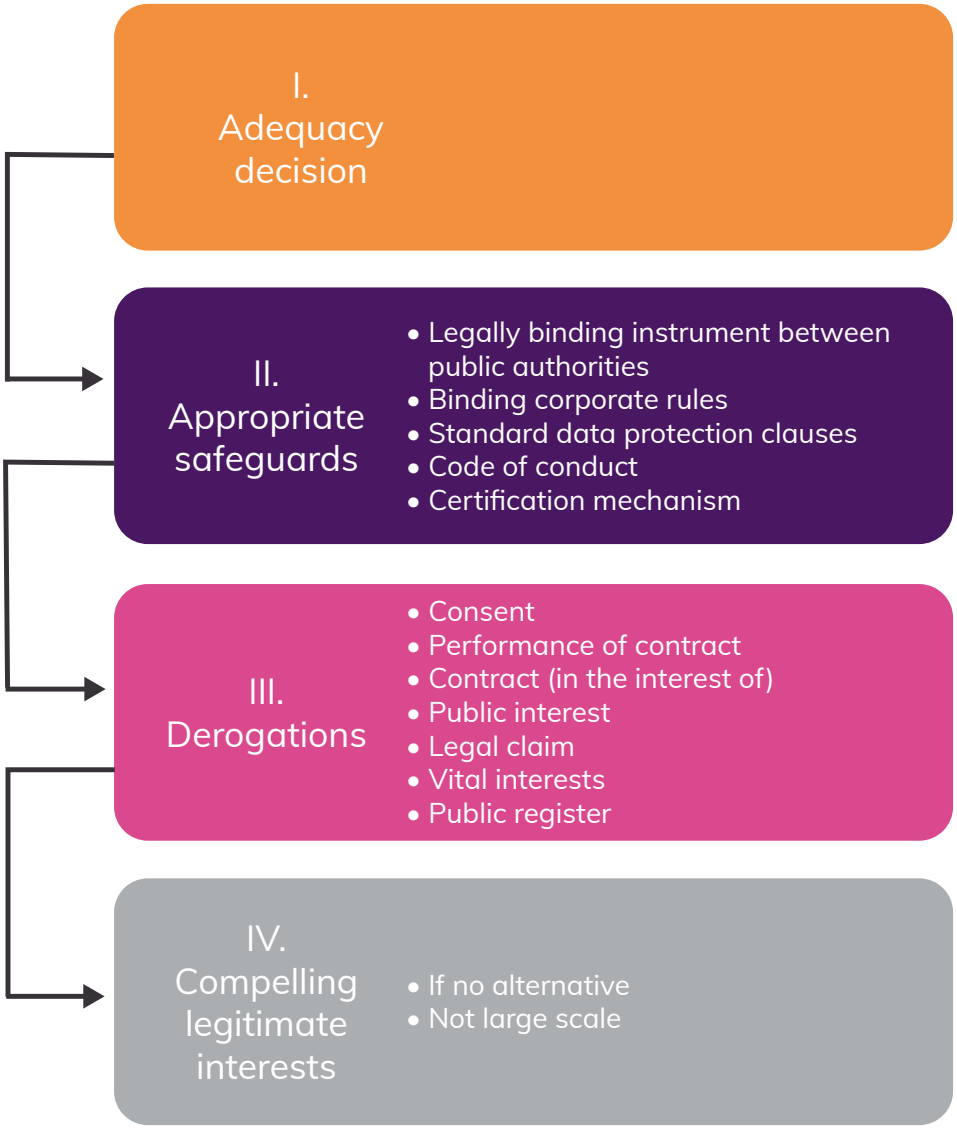
Summary

The GDPR/UK GDPR requires data controllers in the EU/EEA and UK to follow a 'layered approach' to international transfers of personal data, along a hierarchy of measures beginning with adequacy decisions and ending with derogations for exceptional circumstances (see figure below).

However, the CJEU's rulings in the Schrems I and Schrems II cases demonstrates the very high burden that is placed on data controllers to ensure that an acceptable level of protection is provided for the transfer[11]. In some cases this may not be guaranteed through adequacy or appropriate safeguards, which have been shown to be challenging for some forms of genomic and health research, which leaves only exceptional derogations available.

There is potential for positive developments in this area, in particular if codes of conduct can be developed to enable transfers in specific sectors, such as genomic research, or if there are further legislative developments enabling more fundamental changes to occur. For example, although the UK law currently mirrors that of the EU, there is the potential for the UK to develop new transfer mechanisms that are more research-friendly, and to agree adequacy arrangements with a wider range of third countries, although providing for this simultaneously with securing continuing adequacy with the EU may be challenging.

The layered approach' to international transfers



Endnotes

1. For a discussion of this area see chapter seven of the PHG Foundations 2020 report, The GDPR and Genomic Data.

2. By virtue of section 3 of the European Union (Withdrawal Act) 2018, the GDPR (Regulation (EU) 2016/679) was retained in United Kingdom law as "direct EU legislation". However, the effect of the Data Protection, Privacy and Electronic Communications (Amendments Etc.) (EU Exit) Regulations 2019, as amended by the Data Protection, Privacy and Electronic Communications (Amendments Etc.) (EU Exit) Regulations 2020, was, from 1 January 2021, enacted/brought into force immediately to make changes to the retained GDPR, and to refer to it as the "UK GDPR".

3. Case C-362/14 Maximillian Schrems v Data Protection Commissioner (Schrems I) [2015] ECR I-650, para 73.

4. Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems (Case C-311/18) (Schrems II)

5. European Data Protection Board (EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures (Adopted on 10 November 2020) https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

6. For a comprehensive assessment see the report: European Academies Science Advisory Council, the Federation of European Academies of Medicine, and the European Federation of Academies of Sciences and Humanities, International sharing of personal health data for research (2021 ALLEA) Available from https://doi. org/10.26356/IHDT (2021).

7. EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Adopted on 10 November 2020.)

8. Bentzen HB, Castro R, Fears R, Griffin G, ter Meulen V, & Ursin G. (2021). Remove obstacles to sharing health data with researchers outside of the European Union. Nature Medicine, 27(8), 1329–1333. https://doi.org/10.1038/s41591-021-01460-0

9. EDPB. (2018). Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, (May), 1–17. Retrieved from https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

10. See Chapter 7 of: The PHG Foundation, The GDPR and Genomic Data (PHG Foundation 2020) available from https://www.phgfoundation.org/report/the-gdpr-and-genomic-data

11. https://www.phgfoundation.org/discussion/impact-of-schrems-ii-on-genomic-data-sharing

PHG FOUNDATION

making science work for health

The PHG Foundation is a non-profit think tank and a linked exempt charity of the University of Cambridge. Our mission is making science work for health, with a focus on policy to support the application of advances in genomics and related fields for individual and population health.