What is the GDPR?

March 2018

Johan Ordish
johan.ordish@phgfoundation.org

The General Data Protection Regulation (Regulation 2016/679) is an act of the European Union that attempts to harmonise data protection regimes across Member States. The GDPR replaces the Data Protection Directive (DPD). As a regulation, the GDPR is directly applicable in Member States. That is, from its date of publication, the GDPR is automatically incorporated as a part of each Member States' national law. The GDPR is important for healthcare, which relies on the use of personal data.

GDPR essentials

- Exists to harmonize and strengthen data subject rights
- 'Data controllers' and 'data processors' must comply
- Applies to 'personal data' and 'sensitive personal data'
- Takes effect from 25 May 2018

Broadly, the GDPR grants rights to data subjects and imposes duties on data controllers and processors.

Will the GDPR still apply to the UK post-Brexit?

The GDPR remains relevant to post-Brexit UK for two reasons: firstly, the UK Government has made numerous representations that it intends to fully comply with GDPR standards both before and after exit night. Secondly, even if the UK does exit from the European Union (without a transition period) the GDPR will still capture many UK bodies. It will apply if a body is established in the EU; and/or if EU consumers are targeted or monitored. Hence, post-Brexit, most UK bodies will need to be GDPR compliant. This will include hospital trusts, GP practices and any other providers that deal with personal health data.

Data controllers and processors

So the GDPR will apply in the UK, but to what data and to whom?

- **Personal data** is information relating to an identified or identifiable natural person (Article 4(1))
- A **data controller** is a person or body that determines the purposes and means of the 'processing' of 'personal data (Article 4(7))'
- **Processing** is any operation which is performed on personal data (Article 4(2))
- A **data processor** is a person or body that processes personal data on behalf of the controller (Article 4(8))

In combination, the GDPR captures a broad range of operations and organisations. In short, if you process data that could be used to identify an individual, you have to comply with the GDPR and enact the rights it provides to your data subjects or face substantial sanctions.

Legal bases for data processing

If you process personal data you must have a lawful basis to process such data. There are six such legal bases (Article 6). In the context of healthcare and public health, the legal bases most commonly relied upon are:

Consent – if the data subject has given consent to the process for specific purposes

The GDPR requires a high standard if one relies on consent. In particular, Article 4(11) requires that consent be freely given, specific to certain purposes, informed, and an unambiguous indication of the data subject's wishes. Although the GDPR heralded consent as its centrepiece, it is a demanding legal basis to rely on – one that is also particularly vulnerable to the rights of data subjects found below.

Public interest – applies where the processing is necessary to perform a task in the public interest or in the exercise of official authority vested in the controller

Interpretation of this legal basis also makes clear that 'public task' is to be interpreted narrowly and must be laid down by law through statutory, common law, or other legal power (Article 6(3) and Recital 41). This severely curtails the kinds of task that might be thought of as being in the 'public interest.'

Legitimate interests – where the processing is necessary for purposes of the legitimate interests of the controller

This legal basis has broad potential application but any legitimate interests must be balanced against the rights and interests of your data subject, which will be interpreted to trump or curtail many of these otherwise 'legitimate' interests.

Special categories of personal data

Processing of certain categories of personal data such as health, genetic or biometric data is prohibited unless an exception applies. Exceptions include where processing is necessary for medical diagnosis, the provision of health or social care, treatment or management of health or social care systems in accordance with law or professional obligations (Article 9(2)(h)). Another exception applies where data processing is necessary for public health and in the public interest (Article 9(2)(i)). Thus, data processing which occurs as part of health or social care service provision or public health a likely to be covered by these exemptions. Data processing for other purposes, for example to support improve wellbeing or to promote a healthier lifestyle may rely on other legal grounds such as the explicit consent of the data subject.

Rights of data subjects

Roughly, if a) the GDPR applies and b) the data held is personal data, data subjects are granted **a package of rights** with which the data controller/processor must comply.

There are eight such rights. A data subject may rectify, erase, or restrict the processing of their personal data; they may access and request 'fair processing information' to give effect to such rights; they may also take their personal data to use with other services and object to processing when their data controller relies on certain legal bases.

The application of these rights under the GDPR is not straightforward. Each right has exceptions and interacts with various legal bases in different ways. Moreover, some rights may be read together to imply another right. The right to explanation is one such constructed right that exists when the following rights are read together.

Right to be informed – data subjects must be provided with 'fair processing information.'

Automated processing – the GDPR has additional protection for where decisions are taken solely by automated means or where automated processing is used for the purposes of profiling.

Is there a right to explanation?

Applying the right to be informed to automated data processing raises the question of whether the Regulation contains a right to explanation and if so, what form this might take.

- The right to explanation potentially provides the data subject with a right to have any decision made by an algorithm regarding their personal data explained to them
- Some algorithms – especially unsupervised machine learning algorithms – are 'black boxes'. In other words, it may be impractical or even impossible to explain exactly why the algorithm came to the decision it did. Hence, if data subjects have a right to explanation, the GDPR may severely curtail the development and use of these algorithms
- If the right to explanation exists, it is not found in any one provision, but rather is constructed from reading multiple provisions together, specifically Articles 13-15, 22, and Recitals 60-63, and 71

Wachter et al. argue that by distinguishing between system functionality, type and timing of decision making, the right explanation 'dissolves' into a right to be informed.[1] If there is merely a right to be informed, this limits what information about the logic and significance of automated decision-making must be provided. Others disagree both with Wachter's conceptual framework and her interpretation that there is no right to explanation.[2]

How algorithms might satisfy a right to explanation

If the GDPR contains a right to explanation, does this mean that the logic of all black box algorithms need to explained? A possible solution is to provide what Wachter et al. have described as 'an unconditional counterfactual explanation'.

By describing the closest scenario in which the outcome sought could be achieved, counterfactual explanations provide a possible solution to the right to explanation/black box dilemma without requiring an understanding of the underlying logic behind the algorithm. However, this approach is legally contested.

Example of counterfactual explanation: mortage

Imagine I apply for a mortgage and am rejected as unsuitable for a mortgage by the bank's algorithm. If I were given an unconditional counterfactual explanation for my rejection, I would be told the smallest change that I would have to make to be eligible for a mortgage. For example: if I earned X amount more, I would have been accepted.

GDPR and healthcare: outstanding questions

- Are some legal bases too narrow and others too wide?
- Does the GDPR contain adequate exceptions for research?
- What impact will the GDPR have on the increasing use of algorithms and software?

PHG Foundation aims to answer these questions and others, through our project, '**Regulating algorithms in healthcare**'.

1. Wachter, S., Mittelstadt, B., Floridi, L. **Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation**. International Data Privacy Law; 2017. 7(2): 76-99.
2. Selbst, A., Powles, J. **Meaningful Information and the Right to Explanation**. International Data Privacy Law; 2017. 7(4): 233-242.
3. Wachter, S., Mittelstadt, B., Russell, C. **Counterfactual Explanation Without Opening the Black Box: Automated Decisions and the GDPR**. Harvard Journal of Law & Technology; 2018.

To find out more, visit:
www.phgfoundation.org/research/regulating-algorithms-in-healthcare

PHG Foundation is a health policy think tank with a special focus on how genomics and other emerging health technologies can provide more effective, personalised healthcare

@PHGFoundation
www.phgfoundation.org