LAWFULLNESS WITHIN THE GDPR:

Understanding data and the GDPR

Student number :208075219 (dyslexia paragraph at the bottom)

This week's content will focus on data processing as it relates to research groups who are involved in scientific health research during this ongoing covid 19 pandemic. This post, being the first of three, will address the main issues by answering a series of questions

This Photo by Unknown Author is licensed under CC BY

1. Are you processing personal data?
2. What is your role? Data processor or controller?
3. What laws apply to you?

This post will work through the following questions in order.

ARE YOU PROCESSING PERSONAL DATA?

Article 4 (1) of the GDPR provides that personal data is any information that may identify a natural person. This data includes "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;"[1] For example, whether someone is tall, short, American with West African ethnicity, has a particular IP address, works at a particular place and so forth, constitutes personal data.

Important to note however, is that there is another type of personal data. According to Article 9 (1)[2] of the GDPR, personal data revealing "*racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing* ***of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health*** *or data concerning a natural person's sex life or sexual orientation*" falls under 'special categories of personal data'.

Furthermore, there is nuance to this data. Information about companies is not personal data, this is because they are not natural persons but legal. The GDPR only covers the private information of natural persons. More so, as highlighted by the Information commissions office, if personal data can be anonymised beyond identifications of people, then it is no longer subject to the UK GDPR. Additionally, data may be Pseudonymised. The ICO maintains however that this is still personal data.

WHAT IS YOUR ROLE? CONTROLLER OR PROCESSOR?

According to the ICO, Controllers are distinguished from processors by the act of decision making. While controllers exercise "overall control over the purposes and means of processing personal data"[3], processors on the other hand, "act on behalf of the relevant controller"[4].

In our situation, there is a health board and underneath it is scientists undergoing research on its behalf, The health board will be seen as the controller and the scientist swill be seen as processors.

What does data processing actually mean? Data processing is when personal data has been operated upon. This may have been done manually or electronically. For example, computers collecting data on website usage to create targeted algorithms.

[1] Regulation (EU) 2016/679 of the European Parliament and council of 27 April 2016 on the free protections of natural persons with regard to personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) [2016] OJ L 119/.
[2] Ibid art 9(1)
[3] Ico.org.uk. 2018. Guide to the UK General Data Protection Regulation (UK GDPR). [online] Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/> [Accessed 10 June 2022].

It has been noted however, that the statute does not give a particularly strict framework, in terms of who is a controller and who is a processor. Its approach has been described as "loose"[5]. Instead, critics argue that the decision should be made on a case-by-case basis, based on what kind of data is in focus and what the purpose of the data is.

WHAT LAWS APPLY TO YOU?

The GDPR applies to all EU states. Article 45 (2)[6] states that it may also apply to third party countries. Since leaving the EU, the UK has assumed the status of a third-party country. Third party countries may be subject to the GDPR and thus maintain free flowing data exchange and processing if the European Commission decide that the country operates data privacy at the standard operated in the EU. This is called an Adequacy decision. Post Brexit, the UK operates privacy laws by maintaining the GDPR as its own, as the `UK GDPR In addition, there is statutory provision in the Data Privacy Act 2018.[7]

In this case, as researchers under the Medical Research Council, (MRC) the best practice is to comply with the UK GDPR and Data protections Act 2018.

[5] Roisin Creghan, Sekou Taylor, How Much Control Makes a Controller (P. D&P 2018) 18 (6) 10-12
[6] Reg 2016/679(n1) art 45 (2)
[7] Data Privacy Act 2018

LAWFULLNESS WITHIN THE GDPR:

Principles, Consent and Rights of data subject

This week's content will focus on the principle of lawfulness within the GDPR. For a wide and thorough understanding, this post will first give an overview of the main principles of the GDPR. The focus will however be on lawfulness. Throughout the blog, we will continuously apply this understanding to the main scenario with the MRC. As we did last week, the method of navigation is through questions. Thus, this week's flowchart is given as such.

I am a Data Subject

1. What are the main principles of the GDPR?
2. What are the concerns with Consent?
3. What are the rights of a data subject and why are they important?

WHAT ARE THE MAIN PRINCIPLES OF THE GDPR?

Article 5 (1)[8] provides that the main principles of the GDPR are *lawfulness, fairness, and transparency*.

The ICO advises that while the three may overlap, it is mandatory to fulfil all of them. "it is not enough to show your processing is lawful if it is fundamentally unfair or too hidden from individuals concerned"[9]. This means that to properly process data in line with the GDPR, great care must be taken to tick all the boxes.

[8] Reg 2016/679(n1) art 5 (1)
[9] Ico.org.uk. 2018. Guide to the UK General Data Protection Regulation (UK GDPR). [online] Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/> [Accessed 10 June 2022].

+ Lawfulness- Before personal data can be processed, one needs to ensure that specific criteria are met. These are called lawful basis. They are set out in Article 6 of the GDPR[10].

+ Fairness- This entails that data should not be used in ways that will cause negative effects. In addition, the data should be processed in a way that is reasonably expected. The ICO however gives nuance to this. It is possible to use personal data to the detriment of a person in a way that is not unfair. The significant thing is whether there is justification. E.g. tax evasion data

+ Transparency- The ICO defines transparency as "being clear, open and honest" with people from the beginning about the who how and the why on the part of the controller.

Circling back to the principle of lawfulness, the lawful bases set out in article 6 are as such;

- Consent
- Contract
- Legal obligation
- Vital Information
- Public Task
- Legitimate interests

In practical application, the ICO details that deciding which basis is appropriate is a matter of what the controller's purpose is. It advises that where more than 1 purpose exists, they should be identified and documented.

Additionally, it highlights the possibility of the choice falling between legitimate interests and consents. It notes that Legitimate interests may be a better option, allowing more control over the data and "responsibility" in line with people's expectations.

Conversely, It is suggested that the consent route may be a safer option where the data controller "prefers to give individuals full control over and responsibility for data" this includes the option to decide against the data processing.

[10] Reg 2016/679 (n1) art 6

WHAT ARE THE CONCERNS WITH CONSENT?

To begin with, we will look at some background to consent. The ICO[11] describes consent as "giving people real choices and control". It adds that 'genuine consent' should put individuals "in charge and build trust and engagement".

The ICO puts it succinctly. However, as we will see, consent is not quite as simple as tea.

Article 7 of the GDPR[12] lists the conditions for consent.

- The consent must be "distinguishable from other matters, in an intelligible and easily accessible form.
- "The data subject shall have the right to withdraw at any time".
- It must be shown that consent is necessary for the contract to hold.

When applied to children, there is slight nuance. Recital 38 states that children are entitled to special protection of their personal data as they are likely to be less aware of the risks, consequences, and safeguards. As such, article 8 of the GDPR entails that processing children's data is only lawful in a situation where consent has been provided by the "holder of parental responsibility"[13].

Important to note is the fact that consent has developed since the old directive. In some ways, it is particularly different in the UK.

- Consent must be separate from other terms and conditions
- Preticked boxes are no longer valid. Instead, continuous, and active opt in is required
- Consent must be given separately to different processing activities
- Third parties must be revealed
- Individuals maintain a right to withdraw consent
- Consent is not freely given where there is a clear power imbalance between individual and controller

[11] Ico.org.uk. 2018. Guide to the UK General Data Protection Regulation (UK GDPR). [online] Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/> [Accessed 10 June 2022].
[12] Reg 2016/679 (n1) art 7
[13] Reg 2016/679 (n1) art 8

Relevant to our health research group is the fact that the ICO has highlighted that for scientific research, "even where an ethical or legal obligation exists to obtain consent from those participating in research,"[14] In a UK GDPR case, consent may still be withdrawn at any time. This means that a research group is no exception

What does this mean for the MRC groups?

This may mean that even after going as far as obtaining consent, the data subjects may still withdraw their consent to their sensitive data being processed. While ethically, it may be important to carry out this research for the quick recovery from the pandemic, the rights of the data subject must be maintained.

Alternatively, the groups may choose a different lawful basis where consent is not vital. This will dispel their consent worries. An example of an alternative lawful basis for data processing that may suit them is public interest as given in article 6.

RIGHTS OF A DATA SUBJECT

This section will look at brief summaries of each right. The rights can be found under articles 16 – 22 of the GDPR.[15]

The rights of a data subject include

- Right to be informed- this is in line with the transparency principle. This makes it possible for individuals to be informed about the use and collection of their data.

- Right of access- This gives people the right to obtain a copy of their data in order to understand why and how the data will be used.

- Right of Ratification- this right place the onus on the individual to ensure the accuracy of data. It allows for individuals to correct and complete inaccurate data.

- Right of erasure -Otherwise known as the right to be forgotten, this was retained from the case of google Spain[16]While not an absolute right as it is subject to factors such as balancing the right to freedom of information, it allows for individuals to request that a data controller erase their data.

[14] Ico.org.uk. 2018. Guide to the UK General Data Protection Regulation (UK GDPR). [online] Available at: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/> [Accessed 10 June 2022].
[15] Reg 2016/679 (n1) art 16-22
[16] Case- 131/12 Google Spain v Mario Costeja Gonzalez [2014] ECLI:EU:C:2014:317

- Right to restrict processing- This is where individuals may request that the processing of their information is restricted. This right applies in situations such as breach.
- Right to data portability- This is where individuals are able to transfer their data to another controller.
- Right to object to data processing- While this is not an absolute right, it can apply fully in some circumstances, such as profiling for direct marketing. Here an individual may have the option to object particular processes.

In conclusion, in terms of consent, the research group may embark on the consent journey with its complexities or, it may choose another lawfulness basis. Nonetheless, with view to the additional information, The MRC should make sure to respect the rights of its data subjects.

Thank you for reading!

Next week's blog will focus on Breach

and remedies within the GDPR, as well as the obligations of a controller.