GDPR: *Implementing additional data protection rules in health research*

GDPR: Implementing additional data protection rules in health research

Data controllers conducting "Health Research" must be conscious of the recent signing of the Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018 (S.I. No. 314/2018), as they introduce material changes to the rules governing how health research can be conducted in Ireland.

WHAT DO THE REGULATIONS SEEK TO ACHIEVE?

The Regulations build on the existing themes of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018, by applying a third layer of specific data protection rules to health research in Ireland.

The mandatory additional requirements for health research were brought about through a consultation process between the Minister for Health and the Data Protection Commission. Significantly, the Regulations were adopted on 8 August 2018, within three months of commencement of the GDPR and the Data Protection Act 2018, illustrating that this is a high priority issue for the government and the Data Protection Commission and likely to be actively enforced.

To the extent that the Regulations are silent on specific aspects of data processing, the GDPR and the Act continue to apply.

The key changes that the Regulations introduce are;

1. defining "Health Research";
2. prescribing a list of "Suitable and Specific Measures" to be taken when processing personal data for Health Research purposes, including that "explicit consent" be obtained; and
3. identifying exceptional circumstances in which the explicit consent of a data subject to the processing of their personal data is not required and laying down a detailed process to be followed in these cases.

SAFEGUARDING THE FUNDAMENTAL RIGHTS AND FREEDOMS OF DATA SUBJECTS

Under Article 9(2)(i) of the GDPR the processing of special categories of data (such as data relating to health) for reasons of public interest in the area of public health is subject to "suitable and specific measures" to safeguard the rights and freedoms of data subjects. Similarly under section 42(1) of the Data Protection Act 2018, the processing of personal data for scientific research purposes is subject to "*suitable and specific measures being taken to safeguard the fundamental rights and freedoms of data subjects*". Section 42(2) goes on to provide that such processing must "*respect the principle of data minimisation*", while Section 42(3) states that such processing should only identify the data subjects to the extent necessary for the scientific research.

Where scientific research involves the processing of special categories of data (such as data relating to health), Article 9(2)(j) of the GDPR requires that such processing must:

1. be proportionate to the aim pursued;
2. respect the essence of the right to data protection; and
3. provide again for "*suitable and specific measures*" to safeguard the fundamental rights and interests of the data subject.

The GDPR does not define "suitable and specific measures" but Section 36(1) of the Act partially does. It provides a non-exhaustive list of "suitable and specific measures" that may be adopted by controllers where personal data is being processed for research purposes under Section 42. However, Section 36(2) also provides for further regulations to be made identifying further suitable and specific measures to those listed in Section 36(1) and/or to specify that certain suitable and specific measures be mandatory in some cases.

WHAT IS 'HEALTH RESEARCH'?

The GDPR contains a number of provisions that apply to health research. For example, the GDPR provides that processing for scientific research purposes should be "*interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research*" (Recital 159 GDPR). In addition, scientific research should be subject to "*appropriate safeguards*" in respect of "*the rights and freedoms of the data*

The broad scope of activities constituting health research is maintained in the Regulations where the term "Health Research" is defined as any of the following scientific research for the purpose of human health:

1. Research with the goal of understanding the normal and abnormal functioning of the human body;
2. Research specifically concerned with developing innovative strategies, products or services to diagnose, treat or prevent disease or injury;
3. Research with the goal of improving the diagnosis, treatment, rehabilitation and palliation of human disease and injury and of improving the health and quality of life of individuals;
4. Research with the goal of improving the efficiency and effectiveness of health professionals and the health care system; and
5. Research with the goal of improving the health of the population as a whole or any part of the population through better understanding of social, cultural, environmental, occupational and economic factors on determining health status.

The Regulations also provide that establishing whether a person is suitable for inclusion in each of the foregoing health research activities shall also constitute Health Research.

subject" under Article 89(1). The Regulations are in effect Ireland's attempt to prescribe "*appropriate safeguards*" in the specific context of health research.

WHO MUST COMPLY?

Regulation 3(1) provides that the obligations under the Regulations only apply to data controllers. Therefore, any research institutions undertaking Health Research as data processors on the instructions of a data controller are not subject to the Regulations. However they do of course remain responsible for compliance with all of the other data processor obligations set out in the GDPR and the Act. Further, given the liability provisions in the GDPR can extend to all controllers and processors involved in the processing in some cases, processors have a vested interest in working closely with their controllers to ensure adherence to the new Regulations.

Controllers should also be aware that, insofar as an activity constitutes Health Research, separate EU and national legislation may apply. For example, Recitals 156 and 161 of GDPR and Regulation 15 of the Regulations make it clear that the relevant provisions of the Clinical Trials Regulation (EU) 536/2014 shall also apply when appropriate.

WHAT ARE SUITABLE AND SPECIFIC MEASURES?

Data controllers engaged in Health Research which involves the processing of any personal data (regardless of whether the data includes individually identifiable health data), are subject to the Regulations and must therefore adopt all of the following suitable and specific measures, as set out in Regulation 3:

1. Ensure that arrangements are in place to ensure that personal data is processed in a manner that does not cause damage or distress to the data subject or is likely to cause damage or distress to the data subject;
2. Put appropriate governance structures in place for carrying out Health Research including:
    - 2.1 ethical approval of Health Research by a research ethics committee;
    - 2.2 specification of the data controllers or processors involved;
    - 2.3 compliance with Article 26 of the GDPR if there are joint controllers;
    - 2.4 specification of persons with whom it is intended to share personal data even where that data is pseudonymised or anonymised (and the purpose of such sharing);
    - 2.5 specification of funders or persons supporting the Health Research project;
    - 2.6 provision of training in data protection law and practice to those carrying out the Health Research;
3. Ensure the following processes and procedures relating to the management and conduct of Health Research are in place;

3.1 assessment of the data protection implications of Health Research. If this assessment indicates a high risk to rights and freedoms of individuals, a data protection impact assessment ("**DPIA**") must be carried out (which in turn must follow the requirements of Articles 35 and 36 of the GDPR);

3.2 compliance with the "*data minimisation*" principle in Article 5(1)(c) of the GDPR;

3.3 controls to limit access to the personal data undergoing processing in order to prevent unauthorised consultation, alteration, disclosure or erasure of personal data;

3.4 controls to log whether and by whom personal data have been consulted, altered, disclosed or erased;

3.5 measures to protect the security of the personal data concerned;

3.6 arrangements to anonymise, archive or destroy personal data once Health Research is completed; and

3.7 other technical and organisational measures to ensure data processing is GDPR-compliant, together with processes for testing and evaluating the effectiveness of such measures.

4. Identify and put in place arrangements to ensure personal data is processed in a transparent manner; and

5. Obtain "***Explicit Consent***" from the data subject prior to commencement of the Health Research.

REQUIREMENT TO OBTAIN EXPLICIT CONSENT

Pursuant to the GDPR definition of "consent" and the guidance provided by the Article 29 Working Party, "explicit consent" is an express statement of consent, usually obtained via a written record, which is freely given, specific, informed, unambiguous and capable of withdrawal at any time. Explicit consent is one of the main lawful bases that can support the processing of special categories of personal data under Article 9 of GDPR.

Under the strict terms of the GDPR, explicit consent is not required if one of the other Article 9 grounds is satisfied, such as Article 9(2)(j), where processing is necessary for health research purposes. However, the Regulations provide that when processing personal data for purposes of Health Research, the explicit consent of the data subject must be obtained in addition to the other suitable and specific measures detailed above.

This is probably the most important change introduced by the Regulations. Traditionally many research institutions would rely solely on informed consent to justify health research, albeit they would apply appropriate safeguards to the data, such as anonymization, IT security measures etc to comply in broad terms with data protection laws. The Regulations now embed a list of very specific suitable and specific measures all of which must be applied to all Health Research projects and these apply in addition to the underlying obligation to obtain explicit consent.

EXCEPTIONS TO EXPLICIT CONSENT REQUIREMENT

Under the Regulations, controllers may seek an exception from the requirement to seek explicit consent via a declaration from a Committee (appointed by the Minister for Health) that the public interest in carrying out this research significantly outweighs the public interest in requiring the explicit consent of the data subject (a "**Committee Declaration**"). However, obtaining a Committee Declaration is a very involved process which is set out in detail in Regulations 5 and 6 of the Regulations.

The relevant steps to take advantage of this exception are dependent on whether the Health Research commenced on, before or after 8 August 2018.

NEW HEALTH RESEARCH COMMENCED ON OR AFTER 8 AUGUST 2018

To seek an exemption in relation to new Health Research activity, the applicant controller must convince the Committee that the public interest is significantly weighted in favour of proceeding with the health research over requiring the explicit consent of the data subject. At a minimum, the application must confirm that a DPIA has been carried out and that ethical approval has been obtained for the health research from a research ethics committee. In addition, Regulation 5(4) sets out a detailed list of additional information that must be provided in support of an application for a Committee Declaration (See Appendix).

Note that the Committee Declaration, if granted, only removes the requirement for the explicit consent of the data subject. All other suitable and specific measures, as set out above, must still be in place in all cases.

EXISTING HEALTH RESEARCH COMMENCED PRIOR TO 8 AUGUST 2018

A slightly different test for a Committee Declaration applies where the relevant Health Research commenced prior to 8 August 2018, but the controller processes or further processes personal data after this date. In these circumstances, the controller must either:

(a) obtain explicit consent of data subject as soon as practicable and no later than 30 April 2019; or

(b) apply for a Committee Declaration that explicit consent from the data subject is not required as:

   a. the public interest in carrying out the health research significantly outweighs the public interest in requiring consent of the data subject; or

   b. the controller had previously obtained the data subject's consent to their personal data being processed for health research purposes in accordance with the old data protection regime (Data Protection Directive 95/46/EC and the Data Protection Acts 1988 and 2003) and this consent has not been withdrawn. In this circumstance, the controller is required to provide written information to Committee stating that they made reasonable efforts to contact data subject seeking to re-obtain their consent.

In addition to carrying out a DPIA, the controller must also fulfil the same conditions as apply to new Health Research projects carried out on or after 8 August 2018 (see Appendix).

THE COMMITTEE DECLARATION

Irrespective of when the relevant Health Research commenced, the Committee has authority to either make a Committee Declaration, with or without conditions, or to refuse the application. The Committee may also revoke a declaration where it is satisfied that the conditions imposed by the Committee have not been met.

Committee Declarations, as well as any appeals against these decisions, will be published on the Committee's website.

CONSEQUENCES OF NON-COMPLIANCE

The Regulations are silent on the sanctions faced by a controller for any breaches of the Regulations. However, pursuant to Articles 82 and 83 of the GDPR and Part 6 of the Act, the full suite of enforcement measures and rights of redress for data subjects under the GDPR and the Act shall apply for breaches of the Regulations. These include the well-publicised GDPR fines of up to €20 million or 4% of worldwide annual turnover as well as rights for data subjects to sue, regardless of whether or not they suffer material damage.

CONCLUSION

For both existing and future Health Research projects, the Regulations emphasise the importance of having informed consent forms in place which meet all of the transparency and consent criteria under the GDPR. In addition, the governance and management of Health Research projects should be reviewed to ensure they meet the new standard of "suitable and specific measures" laid out in the Regulations. All controllers engaged in Health Research in Ireland should therefore review their processing activities against the requirements of the Regulations and, if necessary, consider whether an application for an exception to the explicit consent condition should be made to the new Committee.

Rob Corbet
Partner, Head of Technology & Innovation
Arthur Cox

Appendix

Application for a Committee Declaration

The application must satisfy each of the following conditions:

1. Written confirmation that clearly identifies the lawful basis for processing personal data under Article 6 of the GDPR (usually consent or legitimate interests) **and** identify that the controller has met one of the conditions under Article 9(2) regarding processing of special categories of personal data (usually Scientific Research Purposes under Article 9(2)(j)).
2. Written confirmation that clearly identifies the controller or joint controllers and their division of responsibilities.
3. Written information demonstrating that:
   - 3.1 This Health Research requires personal data of the type specified to be obtained and processed rather than anonymised data;
   - 3.2 Processing of personal data will not cause, or is likely to cause, any damage or distress to the data subject;
   - 3.3 Personal data will only be collected and used as necessary for research objective;
   - 3.4 Personal data will not be disclosed without explicit consent to the disclosure by the data subject or as required by law;
   - 3.5 Suitable and specific measures are in place prior to commencement of health research;
   - 3.6 A data protection officer has been appointed in relation to the health research; and
   - 3.7 Ethical approval from research ethics committee has been received.

The application must also attach a copy of the DPIA with particular reference to possibility of data linkages if necessary and details of consultations with potential data subjects and written information demonstrating that public interest in carrying out health research significantly outweighs the public interest in requiring explicit consent of the data subject, together with a statement setting out reasons why it is not proposed to seek the data subject's consent. (In the case of applications relating to existing health research projects which are based on consent, written information is required demonstrating that the controller has made reasonable efforts to contact the data subject who previously provided their consent in accordance with the pre-GDPR data protection regime for the purposes of reobtaining consent from that data subject).

OUR DATA PROTECTION TEAM

ROB CORBET
PARTNER
+353 1 920 1211
rob.corbet@arthurcox.com

JOHN MENTON
PARTNER, HEAD OF COMMERCIAL
+353 1 920 1205
john.menton@arthurcox.com

PEARSE RYAN
PARTNER
+353 1 920 1180
pearse.ryan@arthurcox.com

COLIN ROONEY
PARTNER
+353 1 920 1194
colin.rooney@arthurcox.com

OLIVIA MULLOOLY
ASSOCIATE
+353 1 920 1060
olivia.mullooly@arthurcox.com

ISEULT MANGAN
OF COUNSEL
+353 1 920 1055
iseult.mangan@arthurcox.com

COLM MAGUIRE
ASSOCIATE
+353 1 920 1416
colm.maguire@arthurcox.com

ANN-MARIE GLYNN
ASSOCIATE
+353 1 920 1081
ann-marie.glynn@arthurcox.com

HUGH MCCARTHY
ASSOCIATE
+353 1 920 1324
hugh.mccarthy@arthurcox.com

CIARA ANDERSON
ASSOCIATE
+353 1 920 1347
ciara.anderson@arthurcox.com

ANDREW COLLINS
CONSULTANT
+353 1 920 1771
andrew.collins@arthurcox.com

Contact Us

Dublin
+353 1 920 1000
dublin@arthurcox.com

Belfast
+44 289 023 0007
belfast@arthurcox.com

London
+44 207 832 0200
london@arthurcox.com

New York
+1 212 782 3294
newyork@arthurcox.com

Silicon Valley
+1 650 943 2330
siliconvalley@arthurcox.com

arthurcox.com