General Data Protection Regulation (GDPR): Public interest, approvals and 'technical and organisational measures'

Guidance note 4

1. Who should read this guidance?

This guidance note is primarily designed to support Data Protection Officers (DPOs) and Research Governance staff within research active public authorities[1]. A decision-tree is provided to help you determine when and how to demonstrate that research complies with 'public interest' tests and demonstrate when relevant ethics approvals are in place. We will also briefly cover some of the 'technical and organisational measures' required when holding and using personal data to support research.

DPO's should work with Research Governance staff to ensure that adequate governance processes are in place. We anticipate that most research active organisations (NHS, University, Research Council etc.) will already have robust research governance systems implemented. The majority of DPO's will be able to rely on these to provide them with appropriate assurance of compliance with public interest tests, and to ensure relevant approvals are in place (when necessary). We envisage that robust existing processes are unlikely to require significant change, to provide adequate GDPR assurance.

Researchers may also find this guidance useful, but they should always work with the relevant local governance teams within their organisations and follow local policy.

2. Introduction

A number of public interest tests and approvals are used throughout the new data protection legislation and common law. The organisation(s) that is/are your Data Controller(s) will need to provide evidence that research activities are considered to be in line with either the public interest or relevant approvals in a number of different legal contexts. You may find that you need more than one piece of evidence to demonstrate your research is in the public interest or adequately approved. The evidence required will depend on the legal context. This guidance note clarifies the types of evidence that can be used to demonstrate 'public interest' or 'approval' in:

1. GDPR and the new Data Protection Act, and
2. common law (confidentiality)

[1] 'Public authorities' are defined in the new Data Protection Act, as those bodies that are subject to freedom of information legislation across the UK. This includes: Universities, NHS and Research Councils/UKRI

If your organisation is holding personal data to support research, it is highly likely that you will also be required to apply appropriate 'technical and organisational measures', in order to have access to specific research exemptions provided in GDPR and the new Data Protection Act. Provision of these exemptions reflects the specific, and often unusual way, in which data are handled in a research context.

DPO's and Research Governance staff are encouraged to use existing governance processes to provide relevant assurances. We suspect that this is not likely to demand major change to well established processes / practices.

3. What you need to know before using the decision-tree

To use the following decision-tree you will need to understand what is meant by the following terms. Definitions of each of the following terms are provided in guidance note 3. If you are still unsure, you should speak to your Data Protection Officer or Research / Information Governance teams.

- Personal data
- Special categories of personal data
- Lawful basis (Article 6 legal reasons to hold personal data)
- Additional conditions to hold and process special categories of personal data (Article 9 conditions). Be aware that confidential information differs from personal data (see the table below for clarification).

Personal data (covered by GDPR and the new Data Protection Act)	**Confidential information (covered by common law)**
Structured information (electronic, written down etc.)	Any information (including un-taped, 'live' conversations)
Identifiable (Is it reasonably likely that someone could identify individuals, if they were motivated to do so?)	Identifiable (Is it reasonably likely that someone could identify individuals, if they were motivated to do so?)
Relates to or is about a living person	Relates to or is about a person, living or dead
	Not in the public domain
	Given with the expectation that it will be kept confidential
Personal data need not be anything sensitive ('special categories of personal data' are the more sensitive personal data)	Usually a degree of sensitivity associated with it

An identifier alone (with no accompanying information) may well not be considered confidential information, it depends what other information you are likely to have access to. (E.g. postal address alone, available in telephone listings etc., may be personal data but cannot be considered confidential information).

4. Decision-tree for evidence required

Will your organisation be holding and / or using personal data to conduct research?

NO → Go to blue filled box* on next page.

YES ↓

Will your organisation be using 'public task' (sometimes referred to as 'task in the public interest') as the lawful basis [Article 6(1)(e)] to hold and use this personal data? (All public authorities[1] are very likely to be using this).

YES → Research must be an incorporated or a statutory purpose of your organisation. E.g. Types of evidence required: **University Charter, NHS Act 2006, NHS (Scotland) Act 1978, Health and Social Care Reform Act (N. Ireland) 2009, Education Reform Act 1988 (for 'new universities'), Universities Scotland Act updated 1956, Higher Education Research Act 2017 (Research Councils / UKRI),** etc…

NO ↓

Will your organisation:

a. Use data for research that was originally collected for another purpose? **or**
b. Store research data long-term? **or**
c. Rely on any of the other research exemptions (e.g. exemptions to participants' rights to rectification, erasure etc.)?

i.e. any activity that is covered by Article 89(1) of GDPR and Clause 19 of the new Data Protection Act.

We expect that these requirements would be relevant for almost all research data (that are 'personal data') regardless of the lawful basis.

YES → Your organisation must ensure that:

- no substantial damage or distress will be caused to the data subject by the research activity **and**
- no significant decisions will be made on the basis of the research data*

*In medical research: if you believe that significant decisions will be made on the basis of research data, you must ensure that the **research has been approved by an NHS REC, or an ethics committee established by a Research Council, charity or university** (as defined in tax law); if you intend to do a., b. or c. as outlined in the previous box.

In addition, be aware…

- In these circumstances, you must also apply appropriate 'technical and organisational measures'. See section 5 below.
- Exemptions to participants' rights: You may also need to conform to additional safeguards. In particular, you need to think what you are offering participants in terms of withdrawal from your study.
- Research as a secondary use for data: be aware that the Data Controlling organisation(s) need to keep data subjects informed of how their data is being used.

NO ↓

Will your organisation be holding and using special categories of personal data to support research?

NO → Go to blue filled box* on next page.

YES ↓

Will your organisation be using the additional condition [provided in Article 9(2)(j)] of 'Scientific and historical research' (Most organisations conducting medical research are likely to be using this).

YES → An additional level of protection is offered to special categories of personal data. Therefore you must provide evidence of a robust governance check, which (at least in part) considers public interest, e.g. **Peer review from a public funder, appropriate ethics committee review, approval from CAG or PBPP** (see next page re. the common law).

NO ↓

Over page – to explore requirements of the common law.

*Will you[2] be accessing confidential information to support your research?

NO → No common law requirements.

YES

Would your participants / potential participants expect you to have access to their confidential information?

- *If you are part of their direct care team (i.e. you have an established relationship with participants) they would not be surprised that you have access to their information. (Follow the 'yes' arrow).*
- *If you obtain consent, having asked if you could access their information, participants would not be surprised that you have access to their information. (Follow the 'yes' arrow).*
- *If people might be surprised that you accessed their information – follow the 'no' arrow.*

YES – Participants expect me to have access to their information → You can access the information.

NO – participants might be surprised if I accessed their information

England and Wales

Research use of patient (and social care) confidential information – you require approval from the HRA Confidentiality Advisory Group (CAG). [Requirement of Confidentiality Of Patient Information Regulations]

Scotland

Research use of patient confidential information – you require approval from the Public Benefit and Privacy Panel (PBPP) or local Caldicott Guardian. [Requirement of Common law]

N. Ireland

Research use of patient (and social care) confidential information – you should consult the Privacy Advisory Committee (PAC). [Currently implementing Health and Social Care (Control of Data Processing) Act (Northern Ireland) 2016]

[2] 'you' refers directly to researchers here, rather than to DPOs. The common law relates to specific people having legitimate access to confidential information as opposed to data protection law which regulates Data Controllers and Processors (in this context likely to be organisations with a nominated DPO).

5. Technical and organisational measures

The decision-tree above uses the term ‘technical and organisational measures’. But what do these refer to? In brief, these measures are over and above the standard security measures / processes Data Controllers put in place to keep personal data safe. They are applied to research data, and not necessarily to data collected for other purposes (e.g. clinical care). They should include:

a. Pseudonymisation of research data

Pseudonymising requires the physical separation of ‘real-world’ identifiers from the rest of the research data. A link is maintained between research data and ‘real-world’ identifiers via a cipher or code. The cipher is kept secure and separate from the research data. Thereby limiting how many people in the research team have access to real-world identifiers, making it more difficult to identify individuals from research data, and so helping to guard against accidental disclosure.

This is established, common practice in research, and should continue to be so. We know that if appropriate precautions are **not** taken, the process of pseudonymisation can increase the risk of inaccurate linkage between relevant data items, samples etc. This is why many research teams will already be relying on Standard Operating Procedures (SOPs), with SOP training and monitoring to ensure that the process is robust and mistakes are minimised. Such approaches to pseudonymising should continue across the research sector, whenever appropriate.

b. Data minimisation

Research should be designed so that the data collected is sufficient to address the research question(s) and to achieve the research objectives. Only data that is needed to achieve these aims should be collected. Research teams must minimise how much data they collect (i.e. minimise the number of participants and the number of data items collected about each participant), as well as minimising the degree of sensitivity associated with the data. In other words, researchers must only collect the data they need.

Research ethics committees and funders have always considered the appropriateness of proposed data collection when they review research protocols. They will continue to do so. Researchers should also ensure that they have appropriate and relevant statistical input into the design of studies. Again this is an existing expectation and should continue in order to aid compliance with the need for data minimisation.