GDPR for Research – An Introduction

Introduction of GDPR is the largest change in data protection legislation for 20 years. Operational guidance around the changes for GDPR has been slow to be released, research is a complicated business and involves many different organisations who need to be in sync with each other on how the legislation is being interpreted and implemented.

The Health Research Authority (HRA) have been working with other research organisations to agree on how to implement changes and providing guidance over the last few months, advising researchers to hold off making amendments that relate to the new legislation until the advice is clear. Their GDPR pages contain a wealth of information.

GDPR relates to ‘personal data’ – this is defined 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.’

What else do I need to be aware of?

The EU General Data Protection Regulation (GDPR) strengthens people rights around how their data is collected, processed and disseminated. It is supplemented with specific UK legislation in the form a new Data Protection Act 2018 which covers specific derogations (gaps left in the EU Regulation for Member States to legislate on). This builds on people’s existing rights under the Data Protection Act 1998.

The HRA have been clear that the GDPR is not being introduced to punish researchers, or to curtail research in any way. In fact research involving humans is encourages and recognised in terms of a number of exemptions within the legislation. Research is an example of where data protection is already taken very seriously and most people adhere to best practice.

Fines

The headline grabbing change in GDPR is the increased fines for data protection breaches of up to 4% of annual global turnover or €20 Million (whichever the greater). This has led to scare stories in the press that organisations will receive massive fines for minor breaches, or have to stop working altogether due to the new legislation. The Information Commissioner’s Office (ICO) have provided some myth busting examples. Although these fines are significant
they are likely to be reserved for serious breaches by organisations that have flouted the law or made no/little effort to comply with the legislation.

<table>
<thead>
<tr>
<th>Data Controller/ Data Processor</th>
</tr>
</thead>
<tbody>
<tr>
<td>‘Data Controller’ means the natural or legal person who alone or jointly with others determines the purpose and means of the processing of personal data;</td>
</tr>
<tr>
<td>‘Data Processor’ means the natural or legal person which processes personal data on behalf of the controller.</td>
</tr>
</tbody>
</table>

GDPR introduces specific obligations on both Data Controllers and Data Processors. This differs to previous legislation, and therefore it is important to understand your role in collecting, processing and disseminating data. Where Data Controllers have data processed on their behalf by Data Processors, a contract must be in place.

Legal Basis

Previously researchers gained consent from participants to collect, store and process personal data. Under GDPR Consent is unlikely to be the correct legal basis for these activities. For the majority of research undertaken by NHS and Academic organisations, the legal basis is likely to be ‘a task in the public interest’, and this legal basis replaces the need to get specific consent for each processing task researchers which to undertake.

Researchers will need to continue to gain consent from participants if they wish to share participant’s data which they would normally consider confidential. For example, to access their medical records, or pass demographic data to NHS Digital.

The HRA have provided clear guidance on what this means for researchers.

Data Protection Breaches

There are new processes for reporting breaches of GDPR/DPA. When a breach is discovered, it must be reported to the ICO ‘without undue delay’, and no later than 72 hours after discovery. Both University Hospitals of Leicester (UHL) and the University of Leicester (UoL) have specific processes for reporting data breaches, these will be updated and available via their intranet. Research data breaches are likely to be a Serious Breach of GCP, therefore the reporting process is via the Sponsors Office for either UHL/UoL and they will ensure that the breach is escalated in line with the organisations process.

This Guidance Note was produced by the GDPR for Research Working Group

The Group has representatives from:
- University of Leicester Research Governance and Information Assurance Teams
- University Hospitals of Leicester Research Governance and Information Governance Teams
- Leicester Clinical Trials Unit
- Leicester Biomedical Research Centre