UNIVERSITY OF LEICESTER

Data Protection (GDPR) Guidance Note No. 12

GDPR and Research (GUIDANCE FOR PRINCIPAL INVESTIGATORS)

Does GDPR apply to your research?

- Data Protection relates to any research that uses **personal data**, including medical and scientific research and research in the social sciences, arts and humanities. If the research you are conducting does not contain any personal data then GDPR will not apply to your research output. However, if you do hold any personal data on living individuals as part of your research then this will need to be assessed for GDPR compliance.
- GDPR does not apply to anonymised data, which does not relate to specific individuals.
- Compliance with GDPR and data protection law is an aspect of best practice for research in the collection and governance of information.

What do you need to do?

As a Principal Investigator you will be responsible for ensuring that your research project is managed in a way compliant with GDPR.

- ☑ You will be responsible for completing a data management plan (DMP). This is an organic document that will help to encourage you to think around what will be done with data and to document how you will manage your data throughout the research activity. Your DMP should include GDPR considerations (See Section 1).
- ☑ You should ensure that a Data Privacy Impact Assessment is carried for your research if applicable (See Section 4).
- ☑ You will need to ensure you identify your lawful basis for processing personal data. Pay particular consideration to any special category (formerly known as sensitive personal) data your process (See Section 2).
- ☑ You will need to ensure you maintain documentation on your data processing. This will include identifying the reason why you are collecting data and any locations/systems that you are using to store data (See Section 3).
- ☑ You should ensure that you only collect data that is necessary to undertake your research. If you do not need the data then don't collect it.
- ☑ You will need to ensure that you have appropriate security in place for the personal data that you are holding (such as encryption) (See Section 5).
- ☑ You will need to ensure that you anonymise personal data that has been collected as soon as possible
- ☑ You will need to ensure that research data can be archived, preserved and made available for future use. This should involve ensuring that appropriate consent considerations have been addressed (See Section 8).
- ☑ You will be responsible for arranging appropriate data sharing agreements or contractual terms in place as part of your research. These should include clear descriptions of how the data will be used, stored, shared, archived etc (See Section 5).
- ☑ You will be responsible for ensuring that any data that is transferred to other parties is done so in a secure manner (See Section 7).
- ☑ You will need to ensure data breaches are reported as soon as you become aware of them (See Section 6).
- ☑ You will be responsible for ensuring that relevant training security training is completed. Please note there are different training options depending on the source of your research data (e.g. NHS data) (See Section 9).

UNIVERSITY OF LEICESTER

Data Protection (GDPR) Guidance Note No. 12

1. Completing a Data Management Plan:

Data Management Plans (sometimes known as data sharing plans) are useful resources to record how you will be managing and organising your research data outputs throughout the research process or activity. More information can be found here.

The University of Leicester has a customised template available on the DMPOnline tool. This can be found at: https://dmponline.dcc.ac.uk/. First time users will need to create an account using their UoL authenticated email address.

2. Understanding lawful basis:

If you are collecting and holding personal data you need to ensure you are holding it under the appropriate lawful basis. For research data the appropriate lawful basis will typically be the 'public task'. If you are holding special category (previously referred to as 'sensitive personal') data (race/ethnicity, physical or mental health, sexual orientation etc.) you will then need to outline an additional condition to process the data. This should be documented and captured in a Privacy Notice and information passed on to gdpr@le.ac.uk. Further information on lawful basis can be found here.

Although consent will be obtained as part of our common law duty of confidence, and requirement for informed consent of research subjects, it is not like to be the primary lawful basis for processing data. If consent is currently used as the primary lawful basis this should be reviewed. Further guidance on consent can be found here.

3. Identifying what personal information you hold:

- The University is required to maintain documentation on its data processing activities (the reasons why personal data is collected and used) and the associated assets (the locations or systems holding that data). If the research you are managing contains personal data you will need to inform the Records Management Service of its existence. This Information Asset Register is hosted within our OneTrust privacy management software and extracts from this on departmental assets are available on request, to obtain an extract please email the Records Management Service.
- Once you have identified your data processing activities and associated assets you can then begin documenting additional factors such as your lawful basis for processing the data, if the information is shared with third parties etc. This documentation will mainly be completed via a OneTrust questionnaire associated with your data processing activity or asset. These will be issued to the appropriate 'owner'

4. Data Protection Impact Assessments:

If you are collecting personal data you should carry out a Data Protection Impact Assessment (DPIA) where that processing is likely to result in a high risk to the rights and freedoms of natural persons. To complete a DPIA please consult the following link for the appropriate forms and processes

5. Storing data securely:

- You should also ensure you have classified and manage your research data according to the University's Data Classification principles.
- You must ensure that any personal data you are collecting/using as part of your research is stored securely. This may involve ensuring that your storage devices (such as laptops and memory sticks) are appropriately encrypted. Further information can be found here. You should also ensure that any paper files that you hold with personal data are stored securely in locked filing cabinets or offices.
- If you are storing your data in a specific piece of software you should ensure that this software has the appropriate security measures in place. This will often be captured as part of the IT procurement process, but if you need further information please contact IT Services.
- You should ensure that any data sharing which is likely to occur as part of your research project is reflected in your research contract. This will include checking that appropriate clauses around data protection and how data will be managed and shared accurately reflect your research activities.

6. Data Breaches

- GDPR introduces new obligations to report breaches to the Information Commissioner's Office (ICO) within 72 hours.
- The University must notify the ICO if a breach would result in a risk to the rights and freedoms of individuals. Reporting to the ICO will be done by Information Assurance Services.
- The University must also notify the individuals themselves if the breach would result in a high risk to the rights and freedoms of those individuals.
- In order to proactively manage breaches you should be clear about what a data breach is therefore it is important to ensure you and your team know how to identify and respond to a breach. Further information on data breaches can be found here.
- When a breach has happened immediately contact Information Assurance Services on ext. 7946; ias@le.ac.uk or the IT service desk on ext. 2253; ithelp@le.ac.uk to report the incident.

7. Transferring Data

There are a number of ways that you can ensure that data is transferred securely to other parties. When working with collaborators IT Services recognises "collaborative workers" as having a direct association with the University. This means that access may be granted to certain IT Services though an External University Account. In addition, the File Drop Service enables data to be shared with University staff and external collaborators.

8. Data archiving and publishing

The majority of research funders have introduced policies on research data management and data sharing. The main expectation is that publicly funded research data are a public good, should be managed appropriately and made openly available (where feasible) with as few restrictions as possible.

By depositing your research data outputs in a digital data archive/repository you will be ensuring that the data will be discoverable, preserved, and accessible for others to use beyond the life of your research project.

In addition, some publishers require that the data on which a publication is based is made available by the author. For more information on this please contact the Research Data Management Team.

UNIVERSITY OF LEICESTER

Data Protection (GDPR) Guidance Note No. 12

9. Have you completed Information Security Training?

The University has a dedicated e-learning module on information security which covers the key principles around managing data securely. This training can be accessed on Blackboard via the following link: Online Training

Some GDPR myth-busting:

I have to get rid of all my old emails

- No, but you should make efforts to review these to ensure that any personal data that you no longer have a valid reason for holding is deleted.

We need consent for all the personal data we process

- Consent should not be relied upon as the lawful basis for holding data
- The emphasis on consent under the common law duty of confidence remains unaltered

GDPR is a complete change from the past

- No, GDPR is an evolution in existing data protection law not a revolution. If you have been complying with the principles of Data Protection GDPR should not be a major concern.

GDPR is like millennium bug, it'll all be fine after May 2018

- No, unlike preparations for millennium bug the steps to support GDPR compliance will be an on-going journey

Further myth busting can be found here.

Further information:

- If you need further information or have questions about the implications of data protection legislation on your research please email gdpr@le.ac.uk
- If you need further information on research data sharing and publishing contact researchdata@le.ac.uk
- If you need more information around contractual arrangements and research please email red-contracts@le.ac.uk
- If you need more information around your research and potential IT requirements please email ithelp@le.ac.uk
- Further guidance on data protection legislation is available at: https://www.le.ac.uk/gdpr