UK Research and Innovation (UKRI) Data Protection Policy

Contents

Policy Statement

UK Research and Innovation understands the importance of protecting personal information and is committed to complying with the General Data Protection Regulation 2016/679 (GDPR). It is committed to fostering a culture of transparency and accountability by demonstrating compliance with the principles set out in the Regulation.

GDPR sets out the rules for how organisations must process personal data and sensitive personal data about living individuals. It gives individuals the right to find out what personal data is held about them by organisations and to request to see, correct or erase personal data held.

UK Research and Innovation needs to collect and process personal data about the people (including employees and individuals) it interacts with to carry out its business effectively.

UK Research and Innovation is committed to ensuring that employees are appropriately trained and supported to achieve compliance with GDPR.

1 Policy scope

1.1 This policy applies to all personal data and special category personal data collected and processed by UK Research and Innovation in the conduct of its business and applies to both automated personal data and to manual filing systems.

1.2 This policy applies to all UK Research and Innovation employees, whether permanent, temporary, contractors, consultants or secondees.

2 Personal data definitions

2.1 Personal data is defined in the GDPR:

> **Personal data** means any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
>
> **Special categories of personal data** relate to 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.

3 Data protection principles

3.1 GDPR outlines six principles which underpin the handling of personal data. To ensure compliance with the Regulation, UK Research and Innovation must ensure that personal data is:

(a) Processed lawfully, fairly and in a transparent manner (**lawfulness, fairness and transparency**). In practice this means:
- Having a legitimate ground for collecting and using personal data.
- Not using personal data in a way that would have an adverse effect on the individual concerned.
- Being transparent about how you intend to use personal data and provide privacy notices where appropriate.
- Handling personal data in a way that the individual would reasonable expect.
- Ensuring that you do nothing unlawful with personal data.

(b) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (**purpose limitation**). In practice this means:
- Being clear about why you are collecting personal data and what you will do with it.
- Providing privacy notices when collecting personal data.
- Ensuring that any additional processing of personal data is fair.

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**data minimisation**). In practice this means:
- Only processing the personal data that is necessary.

(d) Accurate and, where necessary, kept up to date (**accurate**). In practice this means:
- Taking reasonable steps to ensure the accuracy of any personal data held.
- Ensuring that the source of the personal data is clear.
- Carefully considering any challenges to the accuracy of personal data.
- Considering whether it is necessary to update the information.

(e) Not kept for longer than is necessary for the purpose (**storage limitation**). In practice this means:
- Reviewing the length of time you keep personal data for.
- Considering the purpose you hold the personal data for in deciding whether, and how long, you retain it.
- Securely deleting information that is no longer needed.

(f) Processed in a manner that ensures the security of data using appropriate technical and organisational measures against unauthorised or unlawful processing, loss, damage or destruction (**integrity and confidentiality**). In practice this means:
- Designing and organising security to fit the nature of the personal data held and the harm that may result from the breach.
- Ensuring that the right physical and security measures are in place, backed by robust policies and procedures and reliable, well-trained employees.
- Reporting security breaches promptly so that they can be reported to the Information Commissioner's Office within the required 72 hours timescale.

3.2 In addition, the first principle requires that one or more grounds for processing must be satisfied for the processing to take place. Many of these relate to the purpose for which you intend to use the data and the nature of the personal information.

3.3 UK Research and Innovation, as the data controller, is responsible for and able to demonstrate compliance with these principles.

4 Access to personal data

4.1 Employees will have access to personal data only where it is required as part of their functional remit.

4.2 All data subjects (including employees, research funding applicants and others who interact with UK Research and Innovation) are entitled to make a Subject Access Request to ask UK Research and Innovation whether it holds any personal data relating to them and, if so, to be given a description of and a copy of that personal data. Exemptions may apply in certain circumstances.

4.3 Subject Access Requests are co-ordinated by the data protection team.

5 Data sharing

5.1 Personal data will not be transferred outside the European Economic Area unless that country or territory can ensure an adequate level of protection for the rights and freedoms of the data subjects in relation to the processing of their personal data.

5.2 Personal data in any format will not be shared with a third party organisation without a valid business reason, a contract or Data Sharing Agreement in place, or without the data subject's consent.

6 Privacy by design

6.1 UK Research and Innovation is committed to meeting the GDPR requirement to consider data privacy at the initial design stages of a project as well as throughout the lifecycle of the relevant data processing.

6.2 Data Protection Impact Assessments (DPIA) are a key mechanism for meeting this requirement and will be carried out for all new system and ensure that privacy risks are considered at an early stage. They allow an organisation to demonstrate to data subjects and regulators that the personal data will be handled in a responsible way and that the organisation is compliant with the GDPR.

7 Roles and responsibilities

7.1 The UK Research and Innovation Data Protection Officer has overall responsibility for UK Research and Innovation's compliance as a data controller and data processor with the Regulation.

7.2 All employees are responsible for ensuring that they meet the requirements of the Regulation. They should familiarise themselves with this policy and related documents.

8 Policy benefits

8.1 This policy will benefit UK Research and Innovation by:

- Promoting transparency and accountability, and fostering a data protection culture across the organisation.
- Ensuring compliance with the Regulation.
- Ensuring employee confidence and compliance in their processing of personal data, being fully informed and aware of their responsibilities and obligations.
- Reducing the risk of financial penalties (up to €20m) and reputational damage from non-compliance.
- Providing confidence to the UK Research and Innovation community that their personal data is being well managed and ensuring data subjects know how they can access it.

9 Compliance

9.1 Breaches of this policy will be investigated and appropriate actions taken.

10 Associated relevant legislation

- General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)
- Privacy and Electronic Communications (ED Directive) regulations 2003
- Human Rights Act 2004
- Computer Misuse Act 1990
- Crime and Disorder Act 1998
- Disability Discrimination Act 1995

11 Related policies and procedures

- Information Security Policy
- Information Governance Framework
- Records Management Policy
- GDPR Overview
- GDPR Glossary
- Data Protection Impact Assessment Guidance
- Consent Guidelines
- GDPR Guidance – Lawful Basis for Processing

12 Review of policy

12.1 This policy will be regularly reviewed to incorporate any legislative change and at least annually. Trade Unions may request for the policy to be reviewed.

13 Amendment history

Version	Comment	Date	By
0.1	Draft Policy created	July 2017	DH
0.2	Revision post review by information manager	August 2017	DH
0.3	Revision post GDPR Implementation Project Board SRO review	October 2017	DH
1.0	Sign-off by GDPR Implementation Project Board	November 2017	DH
2.0	Revision post review by UKRI Terms & Conditions Working Group	March 2018	DH