UK Statistics Authority Data Protection Policy

Date in force: 25.5.18

Data expires: N/A

Last review date: 25.5.18

Next review date: 25.5.19

Responsible Officer: Ross Young

Author: Jason Riches

Approved by: Data Governance Committee

Scope: UK Statistics Authority

Policy Owner: Ross Young

Version No: 1

Main contact for queries: dpo@statistics.gov.uk

Revision History

This document will be reviewed annually.

Revision date	Previous revision date	Summary of Changes

Table of Contents

1. Introduction

The UK Statistics Authority and it's executive office, the Office for National Statistics process a large quantity of personal data, principally for the purposes of producing aggregate National and official statistics and statistical research, and all of our staff will likely come into contact with it in some way. Whether that's respondent data obtained through mandatory and compulsory surveys, data obtained from administrative sources in the public and private sectors, information we hold on behalf of other organisations or the data we hold about our own staff and stakeholders.
We all have a responsibility to ensure that the personal data we hold is treated with respect, kept secure and confidential at all times, and that we comply with data protection legislation.

2. Background

The **General Data Protection Regulation (GDPR)** is a regulation in European law (2016/679) on data protection and privacy for all living individuals within the European Union. It replaces the 1995 Data Protection Directive, on which the UK's Data Protection Act 1998 was based, but unlike a directive it has direct effect in the UK. The GDPR became law on 25th May 2018.
The **Data Protection Act 2018 (DPA)** is UK legislation which compliments the GDPR by making some specific rules and allowances for the processing of personal data for specific purposes. It also applies the GDPR to those areas not already covered.

2.1. Definitions

Data protection legislation means collectively; the General Data Protection Regulation, and the Data Protection Act 2018.
Personal data means any information relating to an identified or identifiable natural living person.
Data subject means the natural person to which personal data applies
Processing means any operation which is performed on personal data, including storage.
Data controller means a natural person, public authority or other body which determines the purposes and means of the processing of personal data.
Data processor means a natural person, public authority or other body which processes personal data on behalf of the controller.
Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

3. Scope

This Policy applies to all staff, contractors and others working on behalf of UKSA.

This policy applies to all functions and activities undertaken by UKSA that involve the use of personal data.

4. Objectives

To ensure compliance with Data Protection Legislation

5. Principles

The GDPR sets out the principles that must be adhered to for all processing of personal data. Personal data shall be-

1. processed lawfully, fairly and in a transparent manner.

   All processing of personal data shall be in accordance with UK and EU law, and only take place to the extent that one of the following applies-
   1. the data subject has given their consent.
   2. the processing is necessary for the performance of a contract.
   3. the processing is necessary for compliance with a legal obligation.
   4. the processing is necessary to protect the vital interests of the data subject.
   5. the processing is necessary either for a task carried out in the public interest or in the exercise of the data controller's official authority.

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4. accurate and, where necessary, kept up to date.

5. kept in a form that permits identification for no longer than is necessary for the purposes for which the data are processed.

6. processed in a manner that ensures appropriate security of the personal data.

6. Practices

Data protection by design and by default.
UKSA shall ensure that the principles and practises of data protection are built into all processing activities, and that the rights and freedoms of individuals are given due consideration at all times.

Data minimisation.
Personal data shall only be processed where it is necessary to achieve the aims of the organisation. Only the minimum amount of personal data required to achieve the aim shall be used. Personal data shall be de-identified or anonymised at the earliest opportunity and in accordance with best practise.

Data retention.
Personal data shall be held only for so long as they continue to enable or assist UKSA undertake its functions. Personal data shall be disposed of appropriately and in accordance with best practise.

Data security.
UKSA shall implement technical and organisational measures to ensure a level of security appropriate to the personal data being processed. The measures put in place shall be regularly reviewed.

Personal data breaches.
All breaches that present a risk to the rights and freedoms of individuals, as determined by the data Protection Officer, shall be reported to the Information Commissioner at the earliest opportunity and in any event no later than 72 hours from discovery. Where a breach represents a high risk to individuals UKSA shall notify all data subjects concerned.

Data protection impact assessments.
When introducing a new processing activity that is likely to result in a high risk to the rights and freedoms of individuals UKSA business areas will undertake an impact assessment to identify and mitigate those risks, and seek guidance from the Data Protection Officer if required.

Transparency.
ONS will provide data subjects with all the information they require to constitute fair processing, at the point of data collection. Where data are collected from administrative sources this information will be provided to data subjects within one month, unless to do so would be disproportionate effort. In addition, and where possible, such information will also be published on ONS website.

Records of processing.
ONS shall maintain up to date records of all the processing activities it undertakes.

Data subject rights.
ONS shall respond to all requests made by data subjects, in relation to the rights they hold under data protection legislation, within one month.

Consent.
Where ONS relies on consent as a lawful basis for processing that consent shall be fully informed, freely given and as easy to withdraw as to give.

Data processors.
ONS shall only use data processors capable of providing sufficient guarantees in relation to security of personal data and data protection legislation compliance.

Training.
All staff who process personal data will receive adequate and regular training in data protection.

Data protection officer.
ONS will nominate a suitably trained and experienced data protection officer to provide advice and guidance on all matters related to data protection. The data protection officer will be involved in all decisions related to personal data, will report directly to the National Statistician and will have no other duties that may cause a conflict of interest.

The Information Commissioner.
ONS will provide support and assistance as required by the Information Commissioner in the fulfilment of their tasks.

7. Roles and responsibilities

Role	Responsible for:	Accountable to:
National Statistician/Statistics Board	Organisational compliance with data protection legislation	Parliament
Data Protection Officer	To monitor compliance and provide advice and guidance	National Statistician
Legal Services	Providing support to the Data Protection Officer	National Statistician
Chief Security Officer	Ensuring all systems are compliant	National Statistician
KIM Manager	Records management and document storage	Chief Security Officer

8. Compliance

All staff, contractors and others working on behalf of ONS are required to comply with this policy. Compliance with the policy will be monitored by the Data Protection Officer.

Failure to comply may result in disciplinary action in line with the organisation's Discipline Policy.

Staff making a complaint in relation to the application of this policy should refer to the organisation's Grievance Policy.

9. Governance

Policy owner:	Ross Young
Policy approval:	Data Governance Committee (DGC)
Compliance Monitoring:	Data Protection Officer
Review and amendments:	Data Governance Committee (DGC)