UKSA Guidance on the Safeguards of Statistical Processing

The following provides guidance on safeguards that must be employed when processing personal data for statistical purposes. In the absence of these safeguards the special provisions made within the GDPR and the Data Protection Act 2018 for statistical processing will not apply.

Of relevance is Article 89 of GDPR – *Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.* Article 89 allows the UK to provide exemptions from certain data subject rights, in situations where personal data are processed for statistical purposes. These exemptions are within the DPA 2018.

Statistical purposes mean any operation of collection and the processing of personal data necessary for statistical surveys or for the production of statistical results. Those statistical results may further be used for different purposes, including a scientific research purpose. The statistical purpose implies that the result of processing for statistical purposes is not personal data, but aggregate data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person – Recital 162, GDPR

GDPR

> *Processing for … statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner – Article 89(1), GDPR*

Data minimisation is the process of reducing the amount of personal data used to the minimum required to properly fulfil a given purpose. Data held should be periodically reviewed to ensure that it is still needed, and if not, appropriately deleted.

Pseudonymisation is the process by which personal data is reduced to a form that can no longer be attributed to a specific data subject without the use of additional information, provided that such information is kept separately and securely.

The safeguards described here can be divided into technical and organisational measures.

Technical measures

Compliance with technical standards for security (e.g. physical security of areas where data are held, secure IT systems and networks, appropriate use of encrypted storage and communication).

These measures should already be in place, and must be regularly reviewed and, where necessary, updated. Departments should ensure sufficient and up-to-date documentation is available to meet their obligation to demonstrate compliance.

Types of policy and guidance documents could include:

Data Protection Policy
Data Security Policy
Data Retention Policy
Physical Security Policy
Clear Desk Policy
Data breach guidance
Data Protection Impact Assessment guidance
Suitable training for all staff processing personal data
Technical means to support data minimisation, most importantly pseudonymisation technologies.

The GDPR requires that data minimisation be considered at all steps of processing. Data minimisation is the practice of identifying the minimum amount of personal data you need to properly fulfil your purpose e.g. what is the minimum amount of data that you need to hold in an identifiable format to produce the statistical output. Preference should be given to full anonymisation where possible, then to pseudonymisation, and finally to use identifiable data only when essential.

Other technical means for data minimisation and enhanced confidentiality should also be considered, e.g. splitting identifiers from sensitive data fields, restricting access to files or specific fields on a 'need to know' basis and automatic disclosure control software.

Organisational measures

General policies and procedures that protect the data should be employed (e.g. security clearance, 'clear desk' policies, regular access reviews, disclosure control policies).

As with technical measures, these should already be in place, and must be regularly reviewed and updated. The GDPR does not add any new requirements in this area, but departments should ensure sufficient and up-to-date documentation is available to meet their obligation to demonstrate compliance.

Data protection impact assessments, even if not legally required by virtue of the processing being unlikely to result in a high risk to the rights and freedoms of individuals, are still a useful tool and should be considered.

Departments may need to be more proactive than in the past in making a full, well documented assessment at the earliest feasible stage. It will be necessary to show that an assessment has been made and any appropriate actions taken before a new data collection begins, and (proportionately and appropriately) in relation to each separate stage of processing and use.

Such assessments should be made retrospectively for ongoing data collections and uses within a reasonable timescale.

In particular, the assessment at each stage should show that the statistical purpose is valid, that the possibilities for data minimisation have been considered in relation to that specific purpose, processing or use, and that suitable technical and organisational measures have been implemented.

It should be noted that (a) regular consideration of the need for retention of the data, and (b) the effective application of disclosure control is integral to the organisational safeguards that need to be demonstrated.

Data Protection Act 2018

Additional safeguards are required by the Data Protection Act 2018

Such processing does not satisfy the requirement in Article 89(1) of the GDPR for the processing to be subject to appropriate safeguards for the rights and freedoms of the data subject if it is likely to cause substantial damage or substantial distress to a data subject. – Part 2, Chapter 2, Section 19(2)

Such processing does not satisfy that requirement if the processing is carried out for the purposes of measures or decisions with respect to a particular data subject, unless the purposes for which the processing is necessary include the purposes of approved medical research. - Part 2, Chapter 2, Section 19(3), DPA 2018

However, these are similar safeguards to those that applied under the Data Protection Act 1998, and so all Departments should be familiar and comfortable working within them.