Scottish Funding Council

Data Collection and Sharing Policy

Contents

Data Collection and Sharing Policy

Purpose

1. This policy sets out procedures for the collection and sharing of personal data by the Scottish Funding Council (SFC).

Policy statement

2. SFC will ensure that any external data sharing will be done in accordance with data protection legislation and guidance issued by the UK Information Commissioner.

3. Our Data Protection Policy commits SFC to processing personal data in accordance with Data Protection Legislation. As a 'Data Controller', we will not process any personal data without a legal basis, and always in accordance with the data protection principles.

4. SFC shall ensure that appropriate contracts or agreements will be in place for any external data sharing activity.

5. SFC will establish a Data Governance Board to ensure that data collection and sharing is in adherence with this policy.

Data Controllers

6. A Data Controller is the individual or organisation that determines the means and purposes of data processing. In general terms a Data Controller will determine the "who, what, why and how" of the processing.

7. SFC will collect and share data with other Data Controllers, including but not limited to colleges and Scottish Government. In such instances, both SFC and the other organisation are able to determine the means and purposes of processing independently or jointly.

Data Sharing with Data Processors

8. Data Processors are external agencies or persons commissioned by, or acting on behalf of, a 'Data Controller' (SFC is the Data Controller in this instance).

9. Typical examples of a Data Processor include an agency or consultant commissioned by SFC, a survey provider, or a provider of an IT service.

10. Sub-contractors employed by any of SFC's appointed Data Processors who process SFC's data are also considered to be SFC's Data Processors and therefore, as Data Controller, SFC is also responsible for any processing carried out by the sub-contractor.

11. SFC must ensure any sub-contracting is carried out with our full knowledge and agreement and is in line with the conditions set out for the Processor.

Data Sharing with Data Controllers

12. Where SFC shares personal data with another Data Controller, and the means or purposes of that data processing is jointly determined, SFC will ensure that an agreement is in place to ensure the duties and responsibilities of SFC and the other Controller are clearly delineated.

13. Where SFC shares personal data with another Data Controller, and both SFC and the other Controller independently determine the means and purposes of processing, SFC will ensure that there is a mutual agreement that both parties will be independently responsible for complying with Data Protection Legislation.

Data Protection Impact Assessments

14. Conducting a Data Protection Impact Assessments (DPIA) should be considered for any project involving personal data. The decision of whether to carry out a full DPIA should be recorded using Part One of SFC's DPIA template.

15. Additionally, it is a legal requirement to carry out a Data Protection Impact Assessment (DPIA) when SFC is intending to process personal data which is likely to result in a high risk to the data subjects (i.e. the individuals whose data is being processed).

16. The IMGO must be consulted on all DPIAs. Where a high risk to the data subjects cannot be mitigated to a lower risk, the IMGO may be required to first consult with the Information Commissioner's Office prior to the processing of the data.

17. Further guidance on DPIAs can be found in the Data Protection Policy and the DPIA template and guidance.

Data Minimisation

18. The amount of personal data shared or collected by SFC must always be kept to a minimum for what is necessary for the purposes for which it is collected.

19. Whenever collecting and sharing data, an assessment should be made as to the necessity of the data sharing and whether the same aims can be achieved by collecting or sharing a reduced or anonymised data set.

Tendering and procuring of external processing services

20. Staff who are involved with the procurement and tendering of goods and services which may involve the processing of personal data for any purpose must first consult with the SFC Data Governance Board.

21. The Data Governance Board must also be consulted when:

    - Re-drafting of SFC terms and conditions for ICT services, professional services or goods and related is required.
    - Any new SFC terms and conditions for external services are being drafted.
    - Re-drafting of SFC tendering process is required.
    - The contracted Data Processor employs a new sub-contractor.
    - Immediately if any data protection issues arise with a data processor or sub-contractor (for example, loss of data, a breach of Data Protection Legislation, or complaints from data subjects).

Data transfers

22. Once an appropriate agreement is in place, it is also vital that an appropriate method of sharing the data is identified and utilised.

Electronic transfers

23. Electronic transfers of personal data from and to SFC, and between Data Processors, must be secure and with appropriate technical measures such as encryption in place.

24. Integrity of electronic methods of data transfer between Data Processors/Controllers, or between a Data Processor/Controller and SFC, must be agreed to by the IMGO and the Head of ISU at the beginning of a contract or when and as changes in procedure or contract are made. The IMGO must be informed immediately by the Data Processor/Controller of any such changes.

25. SFC currently uses a secure server for the majority of data transfers (personal or anonymous). Wherever possible, staff should use this facility for external transfers of personal data with other Data Processors/Controllers. Contact the Head of ISU for further information regarding this transfer method.

26. Emails between SFC and Data Processors, which contain sensitive or large quantities of personal data should only be sent in exceptional circumstances and must be encrypted. If personal data is received without encryption you must inform your line manager and the IMGO.

27. Guidance on encryption and validation methods can be obtained from ISU. The IMGO or the Head of ISU must be consulted before any new data transfer agreements and procedures are implemented at SFC.

28. Any breaches of data security or data loss must be reported to your line manager and the IMGO immediately. Please read the guidance on Data Incident Procedures for further guidance.

Hardcopy transfers

29. To mitigate against data loss during hardcopy transfer occurring at SFC, hardcopy transfers must only be carried out where absolutely necessary and only then using the strictest and most secure methods available.

30. Points to consider when transferring personal data in hardcopy:

    - Where it is practical, consider anonymising the personal identification data before transfer.
    - If possible, separate personal identification data from the rest of the data and send each part separately.
    - Where appropriate, ensure that personal data is kept in a locked container.

31. Where hardcopy transfers are necessary, the procedure must be validated and agreed by the IMGO or the Head of ISU at the beginning of a contract and if any changes are made to the procedure.

32. When transferring personal data:

    - Transfers of personal data must be on a 'point-to-point' basis. This means transferring the information directly from one processor of data to another. This must be done using a secure, well-established and recognised courier service or by vehicles owned by the Data Processor and driven by their staff.
    - Non personal or anonymised data must be transferred using a secure, well-established and recognised courier service.
    - All postal transfers of personal data must be sent using a recorded delivery service.

33. The IMGO must be informed of any new or ad hoc transfers of personal data into, or from, SFC.

Data Governance Board

34. The Board will develop a Data Governance Board (DGB) which should ensure that data and information held within SFC is understood, valued and well managed. Specifically the DGB will:

    - Help develop and own SFC's data governance model.
    - Review and approve Data Sharing Agreements.
    - Review and approve requests for the collection of additional data.
    - Ensure that we have proper controls on our data – particularly that we have restricted access to personal data.
    - Help develop our policy on retention and archiving of data.

35. The Data Governance Group will establish Terms of Reference for the group, which ensures that SFC's data sharing and collection remain compliant with this policy and relevant data protection legislation.

36. The Board will include representative from all directorates. The Data Protection Officer will be a member of the group, as well as a representative from ISU.

Further Information

37. For guidance or advice on this policy contact the IMGO – Emma Pantel - at epantel@sfc.acuk