SFC General Data Protection Regulation Project Plan

Project Lead: Callum Morrison, Information Management and Governance Officer
Reporting to: Richard Hancock, Assistant Director Strategy
Project Deadline: 25 May 2018

Background

1. The EU General Data Protection Regulation (GDPR) and accompanying UK Data Protection Bill (DP Bill) will introduce a more rigorous data protection regime in the UK. GDPR will come into force on 25 May 2018 and the UK government is seeking to pass the associated DP bill by the same date. The implementation project will focus on the GDPR as it is a final text and underpins the wider data protection reform package.[1] It is essential that the Scottish Funding Council (SFC) ensures that the organisation is compliant with the requirements of this new legislative environment.

2. The GDPR has already been passed and will be directly applicable to the UK from 25 May 2018 regardless of any additional UK legislation. However some of the detail of the new requirements will have to be set in UK law by the DP Bill. It should also be noted that the UK Government have confirmed that GDPR will be implemented regardless preparations for the UK to leave the EU.

Aim

3. The primary aim of the project is to ensure that SFC is GDPR compliant by 25 May 2018. Ensuring that SFC complies with the requirements of data protection reform package will be an ongoing process beyond the implementation date as guidance is developed and enforcement action is taken under the new regulatory environment. However, the project will aim to mitigate the main risks posed by data protection reform prior to the legislative changes coming into force.

Summary

4. The project will have three main phases: assessment, development and implementation, though aspects of each of phase will run concurrently.

[1] In addition to the GDPR and DP Bill a new EU Law Enforcement Directive has been passed (which will not apply to SFC) and a new Privacy and Electronic Communications Regulation has been proposed (which would only have a minor impact for SFC).

Assessment

- Assess current data protection compliance
- Identify areas of weakness
- Audit what personal data is processed by SFC
- Identify what changes need to be made

Development

- Ensure that SFC's policies, procedures and contracts are GDPR compliant
- Review and develop staff training
- Review data processing and sharing
- Review how we record and communicate what data we process

Implementation

- Staff training to be delivered
- Policies and procedures to be approved by management
- Data Processing Contracts to be agreed
- Communication of changes to SFC staff

5. Given that there are a number of unknown aspects to the project, the plan will need to adapt as new challenges are identified. The plan will therefore be kept under review by the Information Management and Governance Officer for the duration of the project.

6. In addition to the detail of each phase below, Annex 1 to the plan contains an Activity Schedule. The schedule will be used to identify the deadlines for aspects of the project and to track progress made. The schedule also links to relevant section of the GDPR for each action for reference purposes.

Phase one: Assessment

7. Phase 1 will assess the current measures taken by the organisation to achieve data protection compliance. The assessment will then assist with the identification of areas of risk and will establish what personal data SFC processes to allow for GDPR compliance to be achieved.

Compliance Assessment

8. To assess SFC's current level compliance the Information Commissioner's Office (ICO) GDPR Checklist for Data Processors will be used as a template to identify

what measures are currently in place and to identify gaps between current practice and what is required to comply with GDPR. This is a high level assessment so will not provide a detailed analysis but will provide an overview of the current situation with minimal use of time resources.

Actions:

- Complete ICO self-assessment.
- Write a brief report from the findings in the self-assessment to highlight gaps in compliance.
- Create a list of all information management policies SFC has in place.

Data audit and mapping

9. The GDPR requires organisations to hold records on what personal data are processed and to communicate this information clearly with the data subjects so understanding what personal data the organisation processes is essential for compliance.

10. To perform the audit in a timely manner, the Information Management and Governance Officer will meet with key members of each team and complete a questionnaire on what data their teams process.

11. This information will then be transferred into a high level data processing map to provide a basis for the records of processing and to inform SFC's privacy notices.

12. It is also essential that SFC knows where personal data it is responsible for is processed by third parties and if that processing happens outside of the EEA. This includes when personal data is actively shared with external bodies but also where data is hosted by third parties such as on IT systems or external records storage.

Actions:

- Develop a data processing questionnaire/checklist for staff.
- Meet with key members from each team at SFC to establish what personal data is processed and for what purposes.
- Create data flow maps.
- Identify third party data processors (and if they process data outside of the EEA).

Phase two: Development

13. The development phase will build on the gaps in current practice identified during the assessment stage. The policies, procedures, data sharing agreements and documentation that underpins SFC's data protection compliance will be reviewed and brought into line with the requirements of GDPR.

Records of processing

14. GDPR will require SFC to hold a record of the personal data it processes as well as details such as the purposes and legal conditions for processing. Consideration will need to be given to the best way to record these activities. The records could be held in their own right or could be incorporated into existing records such as the Information Asset Register or Retention Schedule.

Actions:

- Assess the most suitable format for records of processing.
- Develop records of processing.

Breach Reporting

15. GDPR will require organisations to report any data breach to the Information Commissioners Office that is likely to result in a risk to people's rights and freedoms within 72 hours of the organisation becoming aware of the breach. Fines for breaches of data protection regulations have increased from £500,000 to €20 Million for most serious breaches. Enforcement will also become stricter under GDPR with fines now being available not only for data losses but other compliance failures such as failing to report a breach.

16. Although the ICO is likely to be proportionate in its enforcement, it remains essential that vulnerabilities and incidents are reported quickly and consistently. SFC should identify the IMGO as the key contact for breach reporting.

Actions:

- Review data breach procedures.

Privacy by design

17. It has been best practice to consider privacy when undertaking projects under the current Data Protection Act, but the GDPR will make it a legal requirement to conduct Data Protection Impact Assessments (DPIA) when considering any 'high risk' processing. The EU Article 29 Working Party on Data Protection has

developed guidance on DPIAs and SFC Privacy Impact Assessment templates should be revised to bring it in line with the working party's guidance. Staff should be made aware of the circumstances in which a DPIA is required and key staff members should receive training on how to conduct them.

18. SFC should also review its current use of personal data and seek to identify where the use of personal data could be minimised or have the data pseudonymised in order to minimise data protection risks.

Actions:

- Develop a Data Protection Impact Assessment template and guidance for staff.
- Consider where data minimisation or pseudonymisation is practical to reduce privacy impact on data processing.
- Consider implementing automatic email deletion.

Privacy notices

19. Articles 12-14 of GDPR require privacy notices to be more granular than under current legislation. To comply, SFC will need to review its current privacy notices and consider solutions to ensure that privacy notices are both easily understood and contain the level of detail required by the regulations. SFC should use a layered approach to privacy notices using simplified to ensure that the information is easily intelligible but with more comprehensive policies with the granular detail required.

Actions:

- Re-write privacy notices.
- Consider the best ways of communicating these internally and externally.

Policy review

20. All information governance policies should be reviewed to ensure they reflect the new requirements of GDPR. The review should prioritise of key policies such as its Data Protection Policy, Information Request Procedures etc. Shortened guidance documentation should also be reviewed with consideration given to consolidating this documentation for ease of use. Policies and procedures managed by other departments may also need to be reviewed to ensure these are GDPR compliant, particularly within Human Resources.

Actions:

- Review all information management policies.
- Consider condensing the guidance documents.

- Assess roles and responsibilities under GDPR.
- Approach other areas of the organisation to ask if any policies relate to the processing of personal data.

Review data sharing agreements

21. Current data sharing arrangements will need to be reviewed to ensure that they are GDPR compliant. Data Processing Contracts will need to have more detail and reflect the changes in the roles of data controller and data processor in the new regulations. Memoranda of understanding may also need reviewed if they relate to the sharing of information between organisations.

Actions:

- Develop template data sharing agreement (consider legal assistance in this).
- Review current data sharing agreements.
- Review procurement.

Develop staff training

22. Ensuring that SFC's staff are trained on the changes in GDPR will be key to ensuring that the organisation complies with the regulations and to implement the changes in practice rather than just achieving paper compliance. Training should be relevant to the work that staff members do to ensure it isn't perceived as a 'tick box' exercise. The training should focus on roles and responsibilities in the workplace rather than legislation to ensure maximum levels of engagement. Training should highlight the role of the Data Protection Officer and promote the reviewed guidance.

Actions:

- Consider best delivery method for training staff.
- Develop training content.

Develop communications plan

23. A communications plan shall be developed to keep staff up to date with changes being made and to communicate the key messages about GDPR. Communications should keep staff up to date with both the project developments and the key changes brought about by GDPR.

Actions:

- Develop an internal communications plan.

Review any use of consent as a basis for processing

24. The requirements for using consent for a basis of processing have changed under GDPR. Any use of consent for the basis of processing personal data should be reviewed. Consideration should be given to using other conditions for processing if they are applicable. If there are not any alternative conditions for processing then the process for obtaining and recording and withdrawing consent should be reviewed.

Actions:

- Review conditions of processing where consent is used.
- Where consent is appropriate, ensure that the conditions of GDPR are met.

Ensure security measures are GDPR compliant

25. GDPR specifies that appropriate security measures should be in place to protect personal data that is processed. These technical measures should also be included in the records of processing where appropriate (e.g. where there is no risk to security by revealing the measures taken to protect data.)

Actions:

- Discuss security measures in place with IT.
- Record these measures within the records of personal data processing.

Phase three: Implementation

26. The third phase is ensuring that the changes made in the development phase are properly implemented

Deliver staff training

27. The staff training developed should be delivered to all current members of staff at SFC. All staff should have completed the training by the 25 May 2018.

Actions:

- Deliver training to SFC staff – detail TBC.

Communicate changes to staff

28. In accordance with the communications plan, key messages and progress updates should be communicated to members of staff.

Actions:

- TBC.

Updated policies and procedures approved by Chief Operating Officer

29. Changes to policies and procedures to be reviewed by the COO and any relevant changes made ahead of 25 May 2018. Policies to be implemented on 25 May 2018.

Actions:

- TBC.

Data Processing contracts to be agreed

30. Data processing contracts should be agreed with any data processors/joint controllers to ensure that these are GDPR compliant ahead of 25 May 2018.

Data weeding exercise

31. Carry out a data weeding exercise to delete or destroy any personal data that SFC no longer needs to hold. This should be led by key members of staff in each business area ensuring that all forms of data storage are considered.

Actions:

- Communicate guidance to staff on how to carry out a data weeding exercise.

Annex 1: Activity Schedule

NB: The colour filling in the updates cell corresponds to the completion status with: **blue** – complete; **green** – no issues/on track; **amber** – at risk/issues still to be addressed; and **red** – serious concerns/behind schedule

Ref.	Activity	Relevant GDPR articles	Teams to consult	Completion Deadline	Updates
	Phase one: Assessment				
4.1	Complete ICO self-assessment	All	N/A	26/01/2018	15/01/2018 – self assessment completed. Data to be used for below report
	Draft a report to highlight gaps in compliance	All		07/02/2018	07/02/2018 – Report drafted and additional actions added to this GDPR project plan
	Create a list of all information management policies SFC has in place	All		23/01/2018	24/01/2018 – Completed
4.2	Develop a data processing questionnaire/checklist	All		19/01/2018	16/01/2018 – checklist drafted
	Complete data processing questionnaire with key staff	A.12, A.13, A.14, A.30	All teams	To be completed by 09/03/2018	29/01/2018 – CM and RH agreed that this questionnaire should be sent to each director and for them to advise which members of the team to complete. 20/02/2018 – checklist complete and ready for circulation
	Compile a list of third party processors of personal data	A.28, A.29, A.12, A.13, A.14	IT, Data Collection	TBC once data processing questionnaires are returned. Provisionally 16/03/2018	There is a risk that not all third part processors are identified in the staff questionnaire, impacting on elements in the development stage.

	Phase two: Development				
5.1	Assess most appropriate format for Records of Processing	A.30, A.32	Data Collection Team, IT	06/02/2018	06/02/2018 - CM and RH agreed that RoP should be kept alongside the Information Asset Register to reduce excess policy documentation and ensure that these documents can be maintained. The ICO's RoP template has been used as a base for this record.
	Develop Records of Processing (see 5.10 for security measures)	A.30, A.32	IT, Data Collection	23/03/2018 (see 5.10 for security measures)	06/02/2018 - IMGO has started to compile records of processing using the current Information Asset Register. This aspect is reliant on the timely completion of the staff questionnaire.
5.2	Review breach reporting procedures	A.33, A.34	IT	29/03/2018	
5.3	Develop a Data Protection Impact Assessment template	A.35, A.36	IT	06/04/2018	
	Consider if any personal data SFC processes could be anonymised or pseudonymised.	A.25	IT, Data Collection	TBC	This aspect needs firmed up once we have assessed what personal data we hold.
	Work with staff on deleting personal data which is past its required retention date.	A.25	All teams	TBC	This aspect needs firmed up once we have assessed what personal data we hold.
	Develop plan for implementing automated email deletion	A.25	IT, Comms	Meeting to be scheduled for April	Meeting took place on 15/01/2018 to discuss this. Agreed that it would form part of GDPR project. Implementation of automated deletion is unable to be implemented prior to GDPR date but will form part of the ongoing plan for improvement and compliance.

5.4	Review Privacy Notices	A.5, A.12, A.13, A.14	IT, Data Collection	20/04/2018	The method for recording Records of Processing details the necessary elements to be incorporated into privacy notices. This information will be incorporated into privacy notices once ROP are complete. This aspect is reliant on the completion of the records of processing.
	Consider best ways of communicating privacy notices internally and externally	A.12, A.13, A.14	IT, Communications	20/04/2018	Meeting with HR officer agreed that internal privacy notices could be delivered via the meta compliance tool. Meeting with web officer agreed current privacy policy would be updated to cover all external processing (i.e. not SFC staff).
5.5	Review all information management policies which relate to data protection: • Acceptable Use Policy • Information Management Framework • Data Breach Procedure (mentioned separately) • External Data Processing Policy • Data Protection Policy • Information Security Policy • Remote Working Policy • Privacy Policy (mentioned separately) • Retention Schedule	A.5	Data Collections, IT, HR	27/04/2018	High volume of work to be completed but much of the work will be interconnected – i.e. changes to one policy will be reflected in the others.

	Consolidate multiple pieces information management guidance for staff into: • Data Protection: guidance for staff • Freedom of Information: guidance for staff (can be completed after 25/05/2018) • Records management: guidance for staff (can be completed after 25/05/2018)	A.5, A.39	Data Collections, IT, HR	27/04/2018	Data protection guide to be produced by date listed – records management and FOI guidance to follow after May.
	Review roles and responsibilities under GDPR. Specifically to ensure a Data Protection Officer is assigned and that appropriate resources are adequately allocated.	A.37, A.38, A.39	HR	09/03/2018	It has been clarified that the Information Management and Governance Officer will be the assigned Data Protection Officer and that the Chief Operating Officer is the Senior Information Risk Owner. The IMGO has submitted a training request for a training course and exam to be a certified data protection practitioner. This training request has been supported by RH and passed to HR for consideration.
	Assist other departments with any necessary reviews of policies that relate to the processing of personal data	A.5, A.39	All	25/05/2018	There is an unknown element to this aspect until staff questionnaire is completed.
5.6	Develop a template data sharing agreement	A.28, A.29	Data collection, legal advice	13/04/2018	Legal advice will need to be sought on this but we will also need to establish what type of contract will be required in advance of going to our lawyers.

	Review current data sharing agreements	A.28, A.29	External stakeholders	13/04/2018	See above.
	Review SFC's terms and conditions for procurement to ensure data protection requirements are correctly stated.	A.28, A.29	Procurement team	13/04/2018	SG revised terms and conditions for procurement will form a good basis for terms and conditions but may need reviewed to suit SFC's needs and wider best practice.
5.7	Consider best delivery method for training of staff	A.39, A.5	HR	01/03/2018	29/01/2018 – Meta Compliance tool will allow for training to be delivered to all members of staff efficiently and without additional cost implications.
	Develop training for staff	A.39, A.5	HR	04/05/2018	This cannot be finalised until policies are re-drafted.
5.8	Develop communications plan	A.12, A.5	Comms team	27/02/2018	Meeting has taken place with the Communications Officer with actions agreed. Plan in progress.
5.9	Review conditions of processing where consent is used	A.7	HR, Comms	29/03/2018	Initial discussions have taken place with the Web Officer regarding consent based processing for newsletters.
	Where consent is appropriate ensure that the conditions of GDPR are met	A.7	HR, Comms	06/04/2018	See above
5.10	Discuss security measures in place with IT	A.32	IT team	20/04/2018	Need to draft summary of required information. Discuss with IT the best way of recording this information.
	Include details in records of processing	A.32	IT team	27/04/2018	See above

	Phase three: Implementation				
	Deliver staff training	A.39, A.5	HR	25/05/2018	There is not a lot of time for implementation of staff training. While training will likely be implemented, there is a risk that not all staff will have completed training in time for GDPR implementation.
	Communicate changes to staff	A.12, A.5	Comms team	25/05/2018	02/02/2018 – A data Protection Blog was published on my SFC to highlight GDPR as a starting point for communications to staff.
	Updated policies and procedures approved by Chief Operating Officer	N/A	SMT	25/05/2018	SFC is on track to have its DP policies reviewed by GDPR implementation date.
	Data Sharing Agreements to be agreed	A.28, A.29	SMT/Board & external stakeholders	25/05/2018	There is a lot of work to be done to get the required groundwork in place before approaching third parties, including all FE to review current agreements. SFC may need to consider prioritising which agreements to get in place accepting some may not be agreed by GDPR implementation date.
	Ensure excess personal data is deleted/destroyed if no longer required.	A.5, A.25	All teams	25/05/2018	SFC has a lot of data stored in its EDRM, two shared drives, Iron Mountain and unstructured data on individual Outlook accounts and desktops. It is likely that retention schedules will not successfully be applied to the majority of this data by 25/05/2018. This work should continually be reviewed and advocated for after 25/05/2018.