Scottish Funding Council
Promoting further and higher education

ACC/18/30
Agenda item 7
11 December 2018

Update on preparations for the General Data Protection Regulation and Data Protection Act 2018

Purpose

1. This paper provides the Audit and Compliance Committee (ACC) with an update on SFC's progress with the General Data Protection Regulation (GDPR) Project.

Background

2. The EU General Data Protection Regulation 2016/679 and associated UK Data Protection Act 2018 (DPA) came into force on 25 May 2018.

3. This legislation introduced a new regime for the processing of personal data, as well as increasing the potential consequences for organisations in cases of non-compliance with the law.

4. The new regime is relevant to SFC because we process personal data, including data of students and staff in Scotland's universities and colleges. We also share data with third parties including other public sector organisations, and private sector organisations.

The Project Plan

5. We developed a GDPR project plan to:

   - Identify the changes that we would need to make to ensure compliance with the new data protection regime
   - Put in place actions and timescale to ensure early compliance.

6. We provided a copy of the Project Plan to ACC on 6 March 2018 for comment.

7. In developing the Project Plan, we focused on tackling the most significant areas of risk to the organisation. However, we recognised that work would continue beyond the implementation date of 25 May 2018. This is in line with comments from the Information Commissioner who has acknowledged that work on GDPR compliance *"…will be expected to continue to identify and address emerging privacy and security risks in the weeks, months and years beyond [25] May 2018*".

Progress and Ongoing Work

8. Appendix 1 of this paper includes the GDPR Activity Schedule, which gives an overview of actions that we have completed, as well as the work we are still undertaking.

9. The Activity Schedule includes the RAG status for each activity: the RAG status relates to the progress made, rather than the level of risk the item presents to the organisation.

10. Overall, we are continuing to make good progress in working through our Project Plan. Some activities have taken longer than anticipated, such as agreeing data sharing agreements with colleges, largely because we chose to work in consultation with college Data Protection Officers to ensure a consistent approach across the sector.

11. Our internal auditors, Scott Moncrieff, undertook an audit of our work on GDPR, which concluded on 5 November. We will provide the Committee with a copy of the report at its next meeting in March 2019, which will provide a degree of independent scrutiny and assurance on our GDPR work.

Risk assessment

12. There is a risk that if we fail to comply with GDPR and the DPA it will result in reputational damage, legal action or an intervention from the Information Commissioner's Office. This paper and the associated GDPR Implementation Project are intended to mitigate the risky working towards full compliance at the earliest opportunity.

Equality and diversity assessment

13. There are no equality and diversity issues associated with this paper.

Recommendations

14. The Audit and Compliance Committee is invited to note this report and comment on progress.

Financial implications

15. There are no direct significant financial implications arising from this paper. However, the executive have incurred modest costs from our running costs budget for advice from our solicitors, Brodies LLP.

Publication

16. This paper will be published on the SFC website.

Further information

17. Contact: Callum Morrison, Information Management and Governance Officer (tel: 0131 313 6566; email: cmorrison@sfc.ac.uk) or Richard Hancock, Assistant Director, Strategy (tel: 0131 6645; email: rhancock@sfc.ac.uk).

Activity	Relevant GDPR articles	Teams	Deadline	Status	Comment
Complete GDPR readiness self-assessment	All	N/A	Complete	**G**	Information Commissioner's Office self-assessment completed. Findings of this report have been used as the basis of the activity schedule shown below.
Draft a report to highlight gaps in compliance	All	N/A	Complete	**G**	Report completed and provided to the Audit and Compliance Committee in February 2018. Additional actions identified in this report were added to this activity schedule.
Create a list of all data protection policies SFC has in place	All	N/A	Complete	**G**	Data protection policies have been identified and listed in the Information Management Framework document.
Develop and complete a data processing questionnaire/checklist	All	All Teams	Complete	**G**	Checklist was developed and sent to key members of staff. Responses were completed and have formed the basis of data mapping work and records of processing to date.
Review Privacy Notices	A.5, A.12, A.13, A.14	ISU, Analysis	Complete	**G**	External privacy notice has been reviewed and is provided publicly on SFC's website. Staff privacy notice has been circulated to all members of staff. We will keep both of these documents under regular review. Staff training is highlighting that privacy notices also need to be provided where new data is collected.

Ensure appropriate privacy notices are communicated internally and externally	A.12, A.13, A.14	ISU, Communications	Complete	**G**	Communicated externally on our website; discussions have taken place with the College sector to ensure that SFC information is included in their privacy notices and to ensure that college students are made aware of the processing that we undertake.
Review roles and responsibilities at SFC to ensure that the organisation complied with requirements under GDPR.	A.37, A.38, A.39	HR	Complete	**G**	The Information Management and Governance Officer (IMGO) is the assigned Data Protection Officer (DPO) and that the Chief Operating Officer is the Senior Information Risk Owner (SIRO). The IMGO has completed a certificated, data protection practitioner course in preparation for the role. These roles have been confirmed in SFC's Information Management Framework.
Ensure there is proper oversight of data protection issues across the organisation.		Analysis, ISU	Complete	**G**	The Senior Management Team agreed to the establishment of a Data Governance Board that will oversee data management within the organisation. It will consist of representatives from across SFC's directorates and will address issues including data sharing, data minimisation and Data Protection Impact Assessments. The first meeting will take place in December 2018.

Communications to staff	A.12, A.5	Communications	Complete	**G**	We have provided briefings to staff at all staff and directorate meetings about the changes to the new data protection regime prior to 25 May 2018. We have also provided a series of email briefings on key points to members of staff in the weeks prior to the implementation date. In addition, our solicitors also provided a briefing on GDPR to all staff on 3 May 2018, which was well attended. The IMGO will continue to provide data protection briefings to staff as part of general duties.
Review where consent is used as a legal basis for processing personal data.	A.7	HR, Communications	Complete	**G**	We have reviewed all aspects of personal data processing where SFC has relied on 'consent'. We have now identified other legal bases, thereby eliminating the need for 'consent' as a basis of processing personal data in the organisation. This minimises the risks to SFC.
Ensure IT security is GDPR compliant.	A.32	ISU	Complete	**G**	We have recently been accredited as compliant with Cyber Essentials Plus. This gives assurance that SFC has appropriate technical measures are in place to ensure compliance. We will still review processes on a case-by-case basis.

Review data protection policies	A.5	Analysis, ISU, HR	Complete	**G**	The IMGO has reviewed and updated all data protection policies, with the exception of SFC's Retention Schedule.
Develop a plan for implementing automated email deletion	A.25	ISU, Communications	31/01/2019	**A**	We have agreed in principle to introduce a process for deleting automatically old emails that are no required for record-keeping purposes. The DPO is currently drafting an implementation plan that will draw on good practice from other organisations. We will agree an implementation plan by 31 January 2019. This action will help to minimise risks to SFC.
Develop records of personal data processing	A.30, A.32	ISU, Analysis	28/02/2019	**A**	We are using the ICO's template as a basis for developing the records of processing. While most aspects of our data processing is recorded, further detail is required in some areas to ensure that we have a full picture of all personal data processed by SFC.

Training for staff	A.39, A.5	HR	31/03/2019	**A**	We started a rolling programme of training of staff in October. A quarter of the organisation have now completed the training programme and the feedback has been positive. We are on target to have all staff trained by 31 March 2019.
Compile a list of third party processors of personal data	A.28, A.29, A.12, A.13, A.14	Analysis,, Finance	31/03/2019	**A**	This work is ongoing, although it is now largely complete. Our Finance team have compiled an external partner list. Our HR and IT providers are recorded separately.
Minimisation of data collected	A.25; A.5	ISU, Analysis	Long term	**A**	This work is ongoing. The college data collections have been analysed for 'necessity' and the data collected has been justified. A similar analysis of HE data collections, which are undertaken by the Higher Education Statistics Agency (HESA), is still to be carried out.

Work with staff on deleting personal data which is past its required retention date.	A.25	ISU, Analysis	Long term	**A**	Work is underway on a team-by-team basis. To encourage this, the DPO has attended directorate meetings and engaged with members of most teams to support implementation of proper retention periods. Our HR function has undertaken a significant amount of work to destroy staff absence records, which have reached their retention limit. We also have historical data stored in our Electronic Document and Records Management System (EDRM), two shared network drives, Iron Mountain offsite storage of records, and unstructured data on individual Microsoft Outlook accounts and desktops. We have identified the largest risks as being with data held by our Outcome Agreement and Analyses teams. Because of the potential volume of work, we may need to establish a separate project to work on data minimisation with additional resources. We will discuss proposals at the first meeting of our new Data Governance Board on 10 December 2018.
Data Protection Guidance	A.5, A.39	ISU, Analysis, HR	Ongoing	**A**	Feedback from staff has indicated that a large data protection guide for staff would not be used often. Instead, we are focusing on providing short regular pieces of guidance on a topic-by-topic basis.

Assist other teams with any necessary reviews of policies that relate to the processing of personal data	A.5, A.39	All	Ongoing	**A**	Where relevant, the DPO has continued to assist other staff and teams to update any SFC guidance or documents with references to personal data. We have not identified any major issues to date.
Review of main Data Sharing Agreements	A.28, A.29	Analysis	Ongoing	**A**	We have prioritised the college data sharing agreements and have been working collaboratively with college Data Protection officers to ensure a consistent approach across the sector. We have made changes to the draft agreement in response to our initial consultation and advice from our solicitors. We are aiming to send final agreements to college principals in December 2018. We are currently negotiating a separate data sharing agreement with the Scottish Government for ESF data. This is taking longer to agree because the Scottish Government wishes to develop a single agreement for use by all ESF Lead Partners. However, we have been active in helping the Scottish Government develop a single template agreement. University sector is collected by HESA: we are in discussions with HESA about the development of a new data sharing agreement which reflects the new data protection regime.

Procurement terms and conditions	A.28, A.29	Finance	TBC	**A**	We have reviewed our terms and conditions for procurement of services. We will commission our solicitors to review our T&Cs, including the data protection aspect for the employment of third party providers. Once we have completed this work, we will request that existing providers sign up to the revised T&Cs.
Review Records Retention Schedule	A.5	All Teams	31/12/2019	**G**	We have a retention schedule in place for our records. We will undertake a review of the schedule in 2019 to ensure it is up to date for the current legal and business environment.