Scottish Funding Council
Promoting further and higher education

ACC/19/24
Agenda item 14
13 June 2019

Update on SFC's General Data Protection Regulation and Data Protection Act 2018 Implementation

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. The legislation introduced a stricter regime for the processing of personal data, as well as increased consequences for failing to comply with the law.

4. The new regime is relevant to SFC because we need to process personal data to carry out our functions as an organisation. As part of this processing we need to share data with third party organisations including colleges, universities and government as well as private sector bodies for the provision of a range of services to SFC.

The Project Plan

5. We developed a GDPR project plan in February 2018 in order 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 have provided updated versions of the Activity Schedule to the Committee in previous meetings.

Progress and ongoing work

7. Overall, we are continuing to make progress in working through our Project Plan. Since the last update to the committee we have:

   - Now delivered training to 91% of the staff team.
   - Worked closely with colleagues in Scottish Government on protocols for sharing personal data for the purposes of providing advice and assistance.

- Reviewed our collection and use of external contacts in line with best practice.

8. Because of the need to balance the GDPR project with other important information governance work, we have had to re-prioritise some of the actions in the project plan.

Risk assessment

9. If SFC fails to comply with data protection legislation there is a risk that it will result in reputational damage, legal action or an intervention from the Information Commissioner's Office. Failure to comply with the law can result in fines of up to €20 million.

10. This paper and the associated GDPR Implementation Project are intended to mitigate risks and guide SFC towards full compliance at the earliest opportunity.

Equality and diversity assessment

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

Recommendations

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

Financial implications

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

Publication

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

Further information

15. 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).

GDPR Activity Schedule

The Activity Schedule includes a RAG status for each activity.

Please note – the RAG status relates to the progress made on deadlines, rather than the level of risk the item presents to the organisation.

G	Complete – tasks labelled green are complete or have been implemented on an ongoing basis
A	To be completed – tasks labelled amber are tasks which are still to be completed but are within the set deadlines.
R	Delayed – tasks labelled red are those which have went beyond their deadline.

Activity		Task	Resource required	Deadline/update	Status
1	**Planning** – background work to assess SFC's position and to inform GDPR Action Plan	Complete Information Commissioner's Officer GDPR readiness self-assessment.	Information Management and Governance Officer (IMGO)	**Complete** – February 2018	**G**
		Draft a GDPR compliance report.	IMGO	**Complete** – provided to the Audit and Compliance Committee in February 2018.	**G**
		Maintain GDPR Action Plan	IMGO – 1 hour per month	**Ongoing** – plan to be kept up to date throughout process	**G**
2	**Resourcing and oversight** – establishing responsibility for data protection within the organisation	Clarify roles and responsibilities at SFC regarding data protection with reference to: • Data Protection Officer • Senior Information Risk Owner	IMGO/ Assistant Director - Strategy	**Complete** – roles now outlined in SFC's Information management framework	**G**
		Establish Data Governance Board (DGB) to provide broader oversight of data protection within the organisation.	IMGO, data collections team and statistics team.	**Complete** – DGB met for the first time 10/12/2018	**G**

Activity		Task	Resource required	Deadline/update	Status
		Data Governance Board to have oversight of the GDPR action plan.	Data Governance Board led by IMGO - 30 mins/month	**Complete –** Action plan to go to the board via email for comment on a monthly basis and to be discussed at each formal meeting.	**G**
		IMGO to provide monthly progress updates to the Chief Operating Officer (COO).	IMGO – 30 mins each month	**Ongoing** – IMGO has started providing these updates	**G**
		IMGO to approximate resources allocated and time required within GDPR Activity Schedule	IMGO	**Complete**	**G**
3	**Communicate updates to staff** – ensure that members of staff are aware of changes in the law and SFC's practice. (See also 'training for staff)	Communicate key messages regarding GDPR implementation ahead of 25/05/2018	IMGO in collaboration with communications team.	**Complete** – key changes communicated in a series of emails and verbal updates to staff ahead of the implementation date	**G**
		Engage staff in determining best format for guidance.	IMGO	**Complete** – Feedback from staff gathered at early data protection training sessions indicated that a text-heavy data protection guide would not be useful.	**G**
		Provide short and regular updates to staff on key data protection issues.	IMGO – 1 hr/ month	**Ongoing** - SFC is providing short updates to staff on key data protection issues by linking them to stories in the news. Although not sent at set intervals, it is intended to send updates approximately once per month.	**G**
		SFC to produce one page 'dos and don'ts' on key data protection issues as a quick reference guide for staff.	IMGO – 1 day	**31/05/2019**. Given the comprehensive staff training activity, this was judged not to be an immediate priority. It is now planned to be completed by **31/07/2019**.	**R**

Activity		Task	Resource required	Deadline/update	Status
4	**Training for staff** - all members of staff to be trained in the essentials of data protection.	Training developed, HR and IT consulted on content, tested on a small group of staff for feedback.	IMGO with input from IT, HR and Assistant Director - Strategy	**Complete**	**G**
		All members of staff to be invited to attend training.	IMGO – 4 hrs (2 remaining training sessions)	**31/03/2019** - Sessions have been running most weeks since November 2018. 67% of staff trained as of 12 March 2019. Average attendance rates have been approximately 60% of number invited.	**G**
		Report on training progress to be provided to the COO with update on number of individuals trained.	IMGO – 30 mins	**Complete**	**G**
		Catch up training sessions to be completed for staff unable to attend initial sessions. Invite to training to be followed up by an email from the COO advising of compulsory nature of training.	IMGO – 6 hours (based on three catch up sessions being required)	**31/05/2019** – Sessions have taken place. 91% of staff have attended training. 5 members of staff have not been trained to date due to calendar conflicts.	**G**
		SMT specific training session to be scheduled.	IMGO – one hour	**31/07/2019 (New entry) –** SMT specific data protection training session to take place.	**A**
		Develop training programme refreshing data protection knowledge of members of staff to be developed with training refreshed on an annual basis. eLearning should be considered as a delivery method.	IMGO – 1 day IT team involvement with use of Meta Compliance software	**31/09/2019**	**A**
5	**Automated email deletion** – emails to be	Draft proposal and seek approval from the Senior Management Team.	IMGO/SMT	**Complete** – January 2019	**G**

Activity		Task	Resource required	Deadline/update	Status
	automatically deleted from Outlook if older than 6 months old.	Launch project advising staff of phased implementation, guidance available, and records management drop in sessions.	IMGO – 2 days per month	**31/03/2019**	**G**
		Project completion deadline. Emails to be deleted on a 6 month rolling basis after phased implementation.	IMGO	**31/03/2020**	**A**
6	**Develop records of personal data processing and data flow maps** – the GDPR requires SFC to record what personal data it processes. Data flow mapping allows a better understanding of how the data moves through the organisation.	Conduct initial data questionnaire with all staff to gain a broad understanding of SFC's data processing	IMGO plus time from each team	**Complete** – April 2018	**G**
		Develop SFC records of processing template using ICO template and guidance.	IMGO	**Complete** – records of processing also partially developed	**G**
		Notify Data Governance Board of planned data audit exercise and seek input/support for the project.	IMGO	**Complete**	**G**
		Conduct a granular data audit exercise with each team at SFC identifying one member of each team to be a key contact for the IMGO.	IMGO with support from teams. 40 hours of IMGO time plus 4 hours from each team (including preparation time).	**31/05/2019** This work has been delayed due to other competing priorities but remains high on the agenda for the GDPR project plan. The revised deadline is **31/08/2019**.	**R**
		Incorporate data gathered in audit exercise into data flow maps recording how personal data flows through the organisation.	IMGO – 1 day	**31/07/2019**	**A**
		Incorporate data gathered in audit exercise into the Records of processing template ensuring records meet	IMGO – 2 days	**31/07/2019**	**A**

Activity		Task	Resource required	Deadline/update	Status
		the requirements of the law. Final records shall be verified with the teams responsible for the information.			
7	**Minimisation of data collected** – SFC to ensure that the data it collects is kept to a minimum for the purposes it requires.	College data collections have been analysed for 'necessity' and the current collections have been justified.	Stats team with advice from IMGO	**Complete** - August 2018	**G**
		HE data collections to be analysed for necessity and for HESA to be advised of any data SFC no longer requires	Stats team with assistance from IMGO – 2 days	**31/05/2019** (to be conducted alongside data mapping). The revised deadline is **31/08/2019**.	**R**
		IMGO to work with HR on review of data collected to ensure no excess information is collected.	HR team with assistance from IMGO – 2 days	**31/05/2019** (to be conducted alongside data mapping) . The revised deadline is **31/08/2019**.	**R**
8	**Data retention** – SFC to ensure that it has an appropriate data retention policy and that this policy is consistently applied.	Review Retention Schedule as part of wider data mapping exercise. The review should benchmark SFC's retention schedules against other retention schedules	IMGO – 5 days	**31/08/2019**	**A**
		Review Information Asset Owners and assign them with clear responsibility for oversight of applying records retention in their areas.	IMGO – 5 hours including informing and advising of responsibilities	**31/08/2019**	**A**
		Ask teams to undertake data cleansing exercises in accordance with new retention schedule.	One member of staff from each team – 3 days each. Advice from IMGO – one day	**31/08/2019**	**A**
9	**Data collection and sharing with other Data Controllers** –	Identify key data sharing between SFC and other data controllers.	Stats team with advice from IMGO	**Complete**	**G**

Activity		Task	Resource required	Deadline/update	Status
	ensure that all data collection and sharing between SFC and other data controllers is GDPR compliant (i.e. organisations responsible for their own data processing)	Colleges – Main agreement covering core data sharing	IMGO – one hour (to send further reminders where necessary)	**Complete** Agreements complete with one college still to finalise agreement	**G**
		College –agreement to cover the sharing of European Social Fund (ESF) programme data	IMGO – 1 day Legal advice required on agreement	**31/05/2019** – SFC still seeking finalised parent agreement from SG	**R**
		Scottish Government – agreement between SFC and SG to cover core student data transfers	IMGO	**Complete**	**G**
		Scottish Government – agreement to cover sharing of ESF data	IMGO – 4 hours (may change if additional changes to agreement required) Legal advice may be required.	**31/04/2019** - SFC-SG agreement draft was provided on 23/05/2019 however the draft did not address some of the key concerns raised in February by SFC. This has now been resolved and the agreement has been signed.	**G**
		Education Scotland	Data Collections Team with advice from IMGO – 30 mins	**Complete**	**G**
		SDS – agreement covering leaver destination data collection and sharing	Data Collections Team with assistance from IMGO	**Complete**	**G**
		HESA – agreement to cover SFC's collection of HE data	IMGO – 1 day Legal advice may be required	**Complete/Ongoing** – temporary agreement signed to cover processing until 31/07/2019 when a review will take place.	**G**
10	**Ensure third party data processing is compliant with GDPR** – ensure	Compile comprehensive list of third parties that process data on behalf of SFC. HR, IT and Finance to be asked to provide	HR, IT and Finance with assistance from the IMGO – 3	**31/03/2019** Still awaiting IT and Finance data to be provided. Delay in part	**R**

Activity		Task	Resource required	Deadline/update	Status
	that SFC has appropriate contracts in place with its data processors (i.e. organisations that process personal data on instruction from SFC)	this information.	hours from each team plus 1 hour from IMGO	due to staff turnover. Revised deadline: **31/07/2019**.	
		SFC's lawyers to review standard procurement T&Cs.	Legal advice plus implementation time by Finance team – 3 hours	**Complete**	**G**
		Request all ongoing services to sign up to our revised T&Cs	Finance team with advice from IMGO – 5 hours	**31/05/2019 –** delayed due to changes in Finance staff, which has now been resolved. Revised deadline: **31/07/2019**.	**R**
11	**Data Protection Policies** – review all of SFC's data protection policies	Identify all of SFC's data protection policies.	IMGO	**Complete**	**G**
		IMGO to review policies to bring them in line with GDPR.	IMGO with assistance from Assistant Director - Strategy	**Complete**	**G**
		COO to review and sign off on policies.	COO – 3 hours	**Complete**	**G**
		IMGO to communicate key changes to members of staff with a focus on carrying out Data Protection Impact Assessments	IMGO – 1 hour	**15/04/2019**	**G**
		Keep policies up to date with any changes to ICO guidance or court decisions	IMGO – variable depending on ICO publications and court cases.	**Ongoing**	**G**
12	**Transparency** – ensure that SFC is transparent in its data processing	Draft staff privacy notice detailing HR data processing	HR and IMGO	**Complete**	**G**
		Draft privacy notice for external data subjects and publish on SFC's website	IMGO with input from the data collections team	**Complete**	**G**

Activity		Task	Resource required	Deadline/update	Status
		Conduct a full review of website data collection with Web Officer	Web Officer with input from IMGO – 4 hours	**31/05/2019** (to be conducted alongside data mapping) . Revised deadline: **31/08/2019**.	**R**
		Review privacy statements once more granular data mapping has taken place	IMGO – 3 hours	**31/06/2019**	**A**
13	**IT Security** – ensure that the personal data held on SFC's systems is processed securely	SFC to gain Cyber Essentials Plus accreditation	IT Team	Complete	**G**
		Staff access permissions to be reviewed	IT Team with input from DGB	**31/07/2019 – confirm with IT**	**A**
		Staff on long term absence to have access to systems restricted	IT Team with input from DGB	**31/07/2019 – confirm with IT**	**A**
		IT Team to push IT security messages to the team and conduct phishing tests	IT Team – 2 hours per month	**31/04/2019** – IT finalising software implementation for this work. . Revised deadline: **30/06/2019**.	**R**
14	**Consent** – ensure any data processing conducted on the basis of consent is GDPR compliant	Assess if any of SFC's data processing is based on consent.	IMGO and Web Officer	**Complete** – the vast majority of SFC's processing does not rely on consent to process, only some comms work.	**G**
		Make improvements to SFC's newsletter subscription page to ensure that it appropriately captures consent for marketing purposes.	Web Officer with assistance from IMGO – 5 hours	**Complete**	**G**