Scottish Funding Council
Comhairle Maoineachaidh na h-Alba

ACC/21/33
Agenda item 8
14 December 2021

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

3. The data protection regime is relevant to SFC because we need to process personal data to carry out our functions. 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.

GDPR project plan

4. A copy of our GDPR Project Plan is attached. The plan identifies:

   - The changes that we need to make to ensure compliance with the new data protection regime.
   - The actions and timescales to ensure compliance.

5. Since the last update to the Committee in August 2021 (ACC/21/15), we have:

   - Completed a series of organisation-wide workshops to help establish our record of personal data processing.
   - Completed our record of personal data processing.
   - Developed data flow maps recording personal data flows through the organisation.

6. There are a small number of outstanding actions in the Project Plan, most of which are dependent on progress with our current IT modernisation project and, in particular, the migration to Office 365. None of these are 'critical' actions that present significant risks to SFC and will be addressed as part of the

work to migrate to Office 365.

Risk assessment

7. 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. This paper and the associated GDPR Project Plan are intended to mitigate risks.

Equality and diversity assessment

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

Recommendations

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

Financial implications

10. There are no significant financial implications arising from this paper.

Publication

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

Further information

12. Contact: Emma Pantel, Information Management and Governance Officer (tel: 0131 313 6566; email: epantel@sfc.ac.uk) or Richard Hancock, Assistant Director, Strategy (tel: 0131 6645; email: rhancock@sfc.ac.uk).

ANNEX

GDPR Project Plan

The Project Plan 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 mostly within the set deadlines.
R	Delayed – tasks labelled red are those which have gone beyond their deadline.

Activity		Task	Resource required	Deadline/update	Status
1	**Planning** – background work to assess SFC's position and to inform GDPR Project 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 Project Plan	IMGO – 1 hour per month	**Ongoing** – plan to be kept up to date throughout process. Reviewed periodically by IMGO and Assistant Director, Strategy.	**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	IMGO/Assistant Director - Strategy	**Complete** – roles now outlined in SFC's Information Management Framework, which was presented to the Audit and Compliance Committee in August 2021 (ACC/21/15).	**G**

Activity		Task	Resource required	Deadline/update	Status
		Risk Owner.			
		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. DGB meets regularly to review and discuss on-going data protection within the organisation.	**G**
		Data Governance Board to have oversight of the GDPR action plan.	Data Governance Board led by IMGO - 30 mins/month	**Complete –** Action plan to be reviewed at each formal meeting.	**G**
		IMGO to provide monthly progress updates to the Chief Operating Officer.	IMGO – 30 mins each month	**Ongoing** – IMGO has started providing these updates. Since the departure of the COO in March 2021, updates are now provided to Assistant Director, Strategy.	**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	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.	**G**

Activity		Task	Resource required	Deadline/update	Status
		protection issues.		Although not sent at set intervals, it is intended to send updates regularly to staff. The most recent update was sent to staff in October 2021.	
		SFC to produce one page 'dos and don'ts' on key data protection issues as a quick reference guide for staff.	IMGO – 1 day	**Complete** – completed, provided to staff, and reviewed by IMGO periodically.	**G**
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)	**Complete.**	**G**
		Report on training progress to be provided to the Chief Operating Officer 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 Chief Operating Officer	IMGO – 6 hours (based on three catch up sessions being required)	**Complete** - 31/05/2019. Sessions have taken place. 91% of staff have attended training. Five members of staff have not been trained to date due to calendar conflicts.	**G**

Activity		Task	Resource required	Deadline/update	Status
		advising of compulsory nature of training.			
		SMT specific training session to be scheduled.	IMGO – one hour	**Complete** - online training offered to SMT and Board members.	**G**
		Develop training programme aimed at refreshing the data protection knowledge of staff.	IMGO – 1 day IT team involvement with use of MetaCompliance software	**On Hold** – the current organisation-wide learning and development platform is being reviewed by HR and Information Systems Unit. DP training will be included be an essential part of any new organisation-wide platform.	**R**
5	**Automated email deletion** – emails to be automatically deleted from Outlook if older than 6 months old.	Draft proposal and seek approval from the Senior Management Team.	IMGO/SMT	**Complete** – January 2019.	**G**
		Launch project advising staff of phased implementation, guidance available, and records management drop in sessions.	IMGO – 2 days per month	**Complete** – March 2019.	**G**
		Emails to be deleted on a 6 month rolling basis after phased implementation.	IMGO	**Partially complete -** 31/10/2020. Initial 10 year deadline implemented in September 2019. Completion of the project interrupted by COVID-19 pandemic and is now on hold due to the introduction of Office 365 within the organisation.	**A**
6	**Develop record of personal data**	Conduct initial data questionnaire	IMGO plus time from each team	**Complete** – April 2018.	**G**

Activity		Task	Resource required	Deadline/update	Status
	processing activities (ROPA) 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.	with all staff to gain a broad understanding of SFC's data processing			
		Develop SFC records of processing template using ICO template and guidance.	IMGO	**Complete**.	**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)	**Complete** – November 2021. Our original approach involved asking teams to complete questionnaires about the processing of personal data. This approach did not provide us with a sufficient level of detail. We therefore adopted a revised approach using team workshops to gather the data. The programme of organisation-wide workshops has now been completed.	**G**
		Incorporate data gathered in audit exercise into data flow maps recording how personal data flows through the organisation.	IMGO – 1 day	**Complete.** Completed upon finalising ROPA workshops.	**G**
		Incorporate data gathered in audit exercise into the	IMGO – 2 days	**Complete.** ROPA completed following	**G**

Activity		Task	Resource required	Deadline/update	Status
		Records of processing template ensuring records meet the requirements of the law. Final records shall be verified with the teams responsible for the information.		organisation-wide audit workshops.	
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 (to be conducted alongside data mapping).	Stats team with assistance from IMGO – 2 days	**Complete** – October 2021. Completed as part of the renegotiation of our Data Sharing Agreement with HESA.	**G**
		IMGO to work with HR on review of data collected to ensure no excess information is collected. (to be conducted alongside data mapping.)	HR team with assistance from IMGO – 2 days	**Completed** - 15/07/2021.	**G**
8	**Data retention** – SFC to ensure	Review Retention Schedule as part	IMGO – 5 days	**31/08/2019** – to be carried out in 2021-22 after the data audit is completed and as part of the	**R**

	Activity	Task	Resource required	Deadline/update	Status
	that it has an appropriate data retention policy and that this policy is consistently applied.	of wider data mapping exercise.		work associated with the migration to Office 365.	
		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** – To be carried out once the above is complete.	**R**
		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 revised approach to be developed as part of the migration to Office 365 project.	**R**
9	**Data collection and sharing with other Data Controllers** – 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)	Identify key data sharing between SFC and other data controllers.	Stats team with advice from IMGO	**Complete.**	**G**
		Colleges – Main agreement covering core data sharing	IMGO – one hour (to send further reminders where necessary)	**Complete** - 15/07/2021**.**	**G**
		College – agreement to cover the sharing of European Social Fund (ESF) programme data	IMGO – 1 day Legal advice required on agreement	To be implemented at next review of the main Data Sharing Agreement with colleges.	**G**
		Scottish Government – agreement between SFC and SG to cover core student data transfers	IMGO	**Complete.**	**G**
		Scottish	IMGO – 4 hours	**Complete.**	**G**

Activity		Task	Resource required	Deadline/update	Status
		Government – agreement to cover sharing of ESF data	(may change if additional changes to agreement required) Legal advice may be required.		
		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.**	**G**
10	**Ensure third party data processing is compliant with GDPR** – ensure that SFC has appropriate contracts in place with its data processors (i.e. organisations that process personal data on instruction from SFC)	Compile comprehensive list of third parties that process data on behalf of SFC. HR, IT and Finance to be asked to provide this information.	HR, IT and Finance with assistance from the IMGO – 3 hours from each team plus 1 hour from IMGO	**N/A** – now part of data audit.	**N/A**
		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	**Complete.**	**G**
11	**Data Protection Policies** – review all of	Identify all of SFC's data protection policies.	IMGO	**Complete** – policies reviewed regularly.	**G**

Activity		Task	Resource required	Deadline/update	Status
	SFC's data protection policies	IMGO to review policies to bring them in line with GDPR.	IMGO with assistance from Assistant Director - Strategy	**Complete.**	**G**
		Chief Operating Officer to review and sign off on policies.	Chief Operating Officer – 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	**Complete** - 15/04/2019. Key changes communicated.	**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**
		Conduct a full review of website data collection with Web Officer	Web Officer with input from IMGO – 4 hours	**Complete**	**G**
		Review privacy statements once more granular data mapping has taken place	IMGO – 3 hours	**31/06/2019** – to be completed in 2021-22 after completion of the data audit.	**R**

Activity		Task	Resource required	Deadline/update	Status
13	**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 the consent of data subjects, but on a legal basis.	**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**