



Update on preparations for the General Data Protection Regulation

Purpose

1. To update the Audit and Compliance Committee on SFC's progress on the General Data Protection Regulation (GDPR) Project Plan.

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. These pieces of legislation bring in tighter the restrictions for processing of personal data and provide additional rights to individuals who we hold data about.

The Project Plan

4. SFC processes large volumes of personal data, including data of students and staff in Scotland's universities and colleges. SFC also shares data with third parties including other public sector organisations, as well as the private sector.
5. The GDPR Project Plan identifies the main changes that GDPR will introduce and what actions will need to be made in order to achieve compliance with the new law. This paper was provided to the ACC on 06 March 2018 for comment.
6. The Project Plan aims to tackle the most significant areas of risk while recognising that GDPR compliance work would continue well beyond the implementation date. This is in line with comments from the Information Commissioner who 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.' While reinforcing that the law will apply and be enforced from this date.

Progress and Ongoing Work

7. This section outlines the main areas of work which have been undertaken as part of the GDPR implementation project to date as well as highlighting key areas of ongoing work to achieve compliance.

Data mapping

8. The main focus of the project has been to ensure that SFC has a good understanding of what personal data the organisation collects, stores, uses, shares and destroys. All areas of the organisation have been involved in contributing to the record of what personal data is processed by SFC.
9. SFC now has a record of the core data processing which the organisation carries out. It is essential that SFC continues to keep this under review and updates this record as the organisation changes and progresses.

Privacy Notices

10. SFC has published a comprehensive privacy notice for all external data processing it carries out and has made this available on the corporate website. This allows SFC to meet the transparency requirements of the GDPR.

Data Sharing

11. SFC has been working to review data sharing agreements with key partners including HESA and the colleges. We have worked collaboratively with key stakeholders to progress this work. Our lawyers are currently undertaking work to draft data sharing agreements with the colleges. This piece of work remains a key priority of the GDPR project.
12. As part of the collaborative working with colleges in Scotland, the IMGO has initiated discussions on finding ways to ensure there is consistency and a standard of best practice in data sharing between SFC and the colleges with a view to widen this work out to the wider Further Education Sector.
13. SFC is also undertaking work to identify and record all remaining third party data processors to ensure that data sharing agreements are in place.

Policy

14. The following data protection policies have been identified as the core policies for review. These have been re-drafted to reflect the changes to the legislation:
 - Data Protection Policy
 - Data Breach Policy
 - Data Protection Impact Assessment (Template and Guidance)
 - External Data Processing Policy
 - Information Security Policy
15. These policies are still to have final amendments made to them and to receive

formal approval but will be implemented over the coming months.

16. Additionally SFC has undertaken to review the following policies which are relevant to data protection compliance in the organisation in light of the GDPR:
 - Acceptable Use Policy
 - Remote Working Policy
 - Retention Schedule

Data Protection Officer

17. As a public body SFC is required by the GDPR to appoint a Data Protection Officer (DPO). SFC has confirmed that the Data Protection Officer role will be fulfilled by the Information Management and Governance Officer.
18. The GDPR sets out specifications for the Data Protection Officer role including that they are appropriately trained and qualified. To ensure appropriate training has been provided the Information Management and Governance Officer completed a Data Protection Practitioner Course in May 2018.

Awareness and Training

19. SFC members of staff have been provided with multiple updates on GDPR covering issues such as the data protection principles and data weeding and were sent 10 key GDPR messages on the implementation date.
20. The IMGO has also run multiple catch ups on GDPR with different teams to discuss how GDPR will affect each team's work and what changes may need to be made going forwards.
21. SFC invited Brodie's Lawyers to provide an introduction to the GDPR to SFC staff. The session was optional but well attended with staff from across the organisation attending and feedback from the session was very positive.
22. Mandatory training will also be provided to staff in the coming months in the form of eLearning. We will use MetaCompliance software to deliver this training which will allow the training to be specific to SFC and to evidence compliance for audit purposes.

Risk assessment

23. This paper and the associated GDPR Project Plan are intended to mitigate the risk that SFC is not compliant with the requirements of GDPR and DPA and, therefore, is not handling personal data in line with the new legal and regulatory regime.

Equality and diversity assessment

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

Recommendations

25. The Audit and Compliance Committee is invited to note this report.

Financial implications

26. There are no direct financial implications arising from this paper. However the board should be aware that data protection compliance may have future financial implications.

Publication

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

Further information

28. Contact: Callum Morrison, Information Management and Governance Officer
(tel: 0131 313 6566; email: cmorrison@sfc.ac.uk.)