ISC16D041

Title:	***Data protection reform and preparations for compliance***
Author:	Ellen Paterson, Information policy & compliance manager
Date:	30 May 2017
Circulation:	ISSC – 13 June 2017
Agenda:	ISC16A003
Version:	Draft
Status:	Open

Issue

An update on matters relating to the forthcoming General Data Protection Regulation (GDPR) and the University's progress towards compliance with the Regulation.

Recommendation

Recipients are invited to: Note the report

Resource Implications

Work is being led by ISD (Strategy, Policy & Compliance team) but GDPR compliance will require input from all University departments handling personal data.

Since January's ISSC, ISD has appointed a fixed-term grade 5 Information Compliance Assistant to provide GDPR preparation support. It is not anticipated that additional staff resource will be required, however the volume of work required will have an impact on other duties for the SPC team, and potentially for other parts of ISD and the University-wide network of data protection contacts (approximately 30 individuals).

Risk Implications

As noted previously, failure to comply with GDPR represents a high risk. It will expose the University to fines of up to 4% of annual turnover, or €20m. Fines can be issued for a range of breaches of the Regulation, including data security breaches.

Bringing data handling practices fully into line with GDPR will be difficult for all universities. For UEA, the devolved nature of many of our data processing activities means we cannot be confident that we are starting from a point of full compliance with the existing Data Protection Act. Compliance with the more stringent GDPR will therefore present us with many challenges and we expect to identify more specific risks in the coming months.

Timing of decisions

The GDPR came into force in May 2016 and will apply from 25 May 2018. We should anticipate no grace period from the UK supervisory body (the ICO) after the Regulation comes into effect; we will be expected to be fully compliant from May 2018.

Further Information

- Data protection reform briefing papers have been circulated at the June 2016, October 2016 and January 2017 ISSC meetings
- The Overview of the GDPR, provided by the Information Commissioner: http://tinyurl.com/zqfmm48
- For enquiries about the content of this paper, contact Ellen Paterson, e.paterson@uea.ac.uk, x2431

Background

The Data Protection Act 1998 is due to be replaced by the GDPR. After some uncertainty in the wake of the EU referendum, the Government has now confirmed the Regulation will apply from May 2018. We are now planning our transition to the new legislation to put in place all the changes required for compliance; however, some aspects of the Regulations require clarification and/or guidance from the Government, the UK Information Commissioner[1] and EU Data Protection Board (Article 29 Working Party)[2].

Discussion

The SPC team continues to lead on preparations for GDPR, however resources are limited (<2 FTE) and diverted as required by existing compliance work.

The accompanying Excel document, 'Data protection roadmap' outlines the SPC team work completed to date and planned for the coming months.

While there are many strands to the work underway, the largest single piece of work will be the creation of Records of Processing Activities (ROPA), as required by GDPR Article 30. The ICO suggests undertaking an information audit as step two in their guide to preparing for GDPR[3] and the SPC team will be working with all areas of the University to establish what personal information the University holds.

Although the level of detail expected by the ICO (in compliance with Article 30) is not yet clear, gathering this information in a systematic way will enable SPC to identify data handling risks, where further compliance work is required. For example, drafting or updating of privacy notices, data processing/sharing agreements or improving security measures.

To improve compliance, all staff must know about GDPR and how it will affect their work. SPC have worked with ARM's internal communications officer to draw together a communications strategy, and are also seeking opportunities to brief senior management on how GDPR will impact their teams.

[1] https://ico.org.uk/for-organisations/data-protection-reform/
[2] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
[3] https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf