ISC17D002

Title:	***Data protection reform (GDPR) and preparations for compliance***
Author:	Ellen Paterson, Information policy & compliance manager
Date:	12 October 2017
Circulation:	ISSC – 20 October 2017
Agenda:	ISC17A001
Version:	Draft
Status:	Strictly Confidential

STRICTLY CONFIDENTIAL

Freedom of Information Advisory Note:
Disclosure of the information in this paper may be prejudicial to the University's compliance with the Data Protection Act, conduct of public affairs or commercial interests. Not to be disclosed without consultation with the Vice-Chancellor.

Issue

An update on matters relating to the forthcoming General Data Protection Regulation (GDPR) and the University's progress towards compliance with the Regulation. A specific focus for this paper is to comment on resource limitations and progress towards the required creation of Records of Processing Activities (see Article 30 of the GDPR).

Recommendation

Recipients are invited to:

- Consider the report

Resource Implications

As noted previously, work is being led by two members of staff (one manager, one fixed term assistant) within the Information Compliance team, with involvement from identified data protection contacts across the University.

While this staffing level is likely to be adequate for maintenance of a core data protection service, it has become apparent the current resource will not be sufficient to undertake all development work required to build UEA's data protection compliance to the standard required by GDPR, even within the planned 'awareness raising > mapping > risk identification > advice' approach.

A recent data breach has exposed the resource limitations, generating significant additional work for the team over the past four months. This incident, combined with a general increased awareness of data protection among staff, has led to an increase in 'bread and butter' compliance work, delaying the team's preparations for the new law.

GDPR will also require the University to appoint a Data Protection Officer. A paper outlining the options for this role was drafted by the Information Compliance team in early 2017. The team recommends that appointment of the DPO is resolved prior to May 2018.

Risk Implications

Failure to comply with GDPR represents a high risk. Aside from the large and well-publicised fines, mishandling of data can lead to reputational damage, compensation claims, loss of trust in the organisation, and potential loss of revenue.

Lack of awareness of, or control over, data processing activities exposes the organisation to considerable risk, as it indicates a fundamental lack of data protection governance, at odds with the high 'accountability' standard required by GDPR. It is this risk the information compliance team are seeking to address through the current data mapping exercise.

Timing of decisions

The GDPR came into force in May 2016 and will be implemented from May 2018. The University will be expected to be fully compliant with the Regulation by that date.

Further Information

The Overview of the GDPR, provided by the Information Commissioner: http://tinyurl.com/zqfmm48
The ICO statement on the Data Protection Bill: https://ico.org.uk/for-organisations/data-protection-bill/
For enquiries about the content of this paper, contact Ellen Paterson, e.paterson@uea.ac.uk, x2431

Background

The GDPR has direct effect across all EU member states.

Despite the ongoing Brexit negotiations, the government has signaled a commitment to GDPR. The Regulation forms part of the Data Protection Bill, currently being debated by the House of Lords. The Bill 'fills in the gaps', detailing how GDPR and the Law Enforcement Directive will apply in the UK. We anticipate further months of uncertainty over the particulars of the law, and inevitable delays in the publication of associated guidance from the supervisory body, the ICO.

We are now planning our transition to the new legislation to put in place all the changes required for compliance.

Discussion – Records of Processing Activities

Article 30 of GDPR requires us to create and maintain Records of Processing Activities (ROPA). While we do not yet have external guidance on the level of detail required, we are taking the approach that we can use this obligation as what has been termed an 'ice breaker': a way of identifying not just how and why we are using data, but as a gap analysis, uncovering other compliance risks faced by UEA – e.g. where we require agreements to be put in place, or privacy notices to be drafted.

We are discovering this is a relatively common approach for organisations, particularly where there is no pre-existing monitoring or maintenance of asset registers or similar. In other words, where the organisation is relatively immature, in compliance terms.

This is clearly a large piece of work, and critical to the success of our GDPR preparations. The plan for tackling the work is as follows:

- Scope (by means of a widely distributed questionnaire, seeking basic information about the activities of a unit, team or department)

- Establishing processing activities (face to face interviews, covering all required aspects of ROPA)
- Identifying initial risks (based on information gathered to date)
- Mapping data flows (identifying common systems, processes)
- Remediation of risks
- Maintenance

With only one member of staff focused on this activity we cannot approach all stages at the same time, and are currently working on stages 1-2 with teams across the organization. While this activity is valuable in uncovering gaps and risks, as well as good practice, the team does not have any specialist tools to log and map the information, nor do we have any ways of capturing the processing teams may be unaware of - the 'dark data' held by the University.

Ultimately, while this work may enable us to be nominally compliant with Article 30 alone, the current exercise will provide a snapshot that is incomplete, does not uncover all the associated compliance risks, and will be very difficult to maintain.

Software exists to aid organisations in capturing and recording both types of processing; the known and the unknown, and the Information Compliance team is not the only area of ITCS with an interest in uncovering this information. After an initial investigation into compliance software stalled earlier this year, the team is working Information Security and CIS teams to identify what they would require from mapping tools.

The team is also working with Information Security and FPG to run a full audit of compliance and security risks, looking specifically at the HESA return activity. It is hoped this pilot will build a representative picture of the risks and the measures that are, and could be, taken to reduce these risks.

The information compliance team recommend a more strategic approach to data mapping, and request support from ISSC to pursue this as a fundamental step towards GDPR compliance.

Attachments

- Data breaches update – Jan – Oct 2017 ***[Redacted - out of scope]***
- Compliance search protocol revision ***[Redacted - out of scope]***