**ISC16D012**

| | |
|---|---|
| **Title:** | ***Data protection reform and preparations for compliance*** |
| Author: | Ellen Paterson, Information policy & compliance manager |
| Date: | 05 October 2016 |
| Circulation: | ISSC – 18 October 2016 |
| Agenda: | ISC16A001 |
| Version: | Draft |
| Status: | Open |

---

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

**Recommendation**
Recipients are invited to: Consider the report

**Resource Implications**
Work is being led by ISD but will require input from all departments handling personal data. Increased resource may be required as we move closer to the implementation of the GDPR.

**Risk Implications**
Failure to comply with GDPR will represent a high risk, exposing the University to fines of up to 4% of annual turnover or 20 million euros. Given existing concerns about the security of our systems, data security will need to be a priority for UEA in order to reduce the risk of significant personal data breaches.

To illustrate the risk, TalkTalk were recently fined £400,000 (far less than the likely sanction under GDPR) for failing to prevent the 2015 cyber-attack. The Information Commissioner commented *'TalkTalk's failure to implement the most basic cyber security measures allowed hackers to penetrate TalkTalk's systems with ease. Yes hacking is wrong, but that is not an excuse for companies to abdicate their security obligations. TalkTalk should and could have done more to safeguard its customer information. It did not and we have taken action.'*[1]

**Timing of decisions**
The GDPR came into force in May 2016, and will apply from May 2018.

**Further Information**
See 'Data protection briefing – GDPR' (ISC15D032), circulated at the June 2016 ISSC.
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. We are now planning our transition to the new legislation to put in place all the changes required for compliance.

**Discussion**

***EU referendum vote***

[1] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/

The Regulations are EU law and will directly apply to UK data controllers, as long as the UK remains a part of the EU. One outcome of the referendum in June has been some uncertainty as to the applicability and longevity of GDPR: would it ever apply here, and if so, for how long?

In the immediate aftermath of the vote, the Information Commissioner's Office took a robust stance on the need for the GDPR, or something very like it. Information Rights bloggers noted how this approach was subsequently moderated[2], but in the past week the new Commissioner has called for the country to adopt forthcoming EU data protection laws[3].

The Prime Minister's recent statement on the invocation of Article 50[4] gives us a strong indication that the UK will remain in the EU, and so be subject to GDPR, until at least the end of March 2019. It now seems likely UK Data Controllers will need to comply with GDPR beyond that date[5].

***SPC preparations to date (with reference to requirements in relevant sections of GDPR)***

- March - May 2016: The work of the two Information Policy & Compliance Managers was rebalanced to allow one IPCM to focus more on data protection work *(see Chapter IV, Section 4)*
- May – to date: Self-training on GDPR and identifying external training opportunities *(see Chapter IV, Section 4)*
- June – to date: Gap analysis, showing where we meet / do not meet GDPR requirements, the risk of non-compliance, and where UK may choose to make amendments to law
- June: Creation of data protection reform web page[6] *(see Chapter IV, Section 4, Article 39)*
- June: Creation of web page to help staff find out what to do in the event of a data breach *(see Chapter IV, Section 2)*
- June: Prepared GDPR briefing presentation *(see Chapter IV, Section 4, Article 39)*
- July – August: Established procedures for handling data protection complaints *(see Chapter III)*
- June – to date: Set-up of network of data protection 'champions' across all University departments *(see Chapter IV, Section 4, Article 39)*
- June – to date: review and logging of data processing and data sharing activities *(see Chapter IV, Sections 1 & 2)*
- August – to date: Setting up web guidance on data sharing *(see Chapter IV, Section 2)*
- June – to date: reviewing and logging of University privacy notices *(see Chapter II, Article 7, and Chapter III, Section 2, and Chapter IV, Section 1, Article 30)*

***Plans for the next quarter***

*Training:*

- New CSED data protection training is planned for November and we will also revisit the need for closer monitoring of completion of the online training module.
- SPC staff will also attend external training in GDPR in November.

*Liaison:*

- We have not yet initiated regular meetings with our contacts, but it is expected that a more structured and consistent approach to liaison will bring to light many processing activities which will require attention (e.g. data processor relationships).

*Logging of processing activities:*

- GDPR will require us to maintain a record of processing activities under our responsibility and this is an area which will need considerable development in the coming months.

---

[2] https://2040infolawblog.com/2016/08/26/any-last-requests/

[3] http://www.bbc.co.uk/news/technology-37512419

[4] http://www.bbc.co.uk/news/uk-politics-37532364

[5] https://actnowtraining.wordpress.com/2016/10/03/brexit-article-50-and-the-great-repeal-bill-gdpr-means-gdpr/

[6] https://portal.uea.ac.uk/information-services/strategy-planning-and-compliance/regulations-and-policies/information-regulations-and-policies/data-protection/gdpr