HUMAN RESOURCES

New College Lanarkshire
Skillset for life

Item 6.1 Resources and General Purposes Committee – November 2017

Data Protection Update

Introduction

On 14 April 2016, the European Parliament approved the General Data Protection Regulation (GDPR), which will come into force across all member states on 25 May 2018. GDPR has the stated aim to "harmonise data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organisations across the region approach data privacy" (www.eugdpr.org). Despite the UK's negotiations to leave the European Union, the UK will still be subject to GDPR as a member state at May 2018.

GDPR is the first significant review of data protection legislation in the EU or the UK for at least 20 years and, given the pace of technological change around information systems and ease of data sharing, its effects will be far reaching.

Key Elements of GDPR

For organisations, GDPR strengthens the requirement for an organisation to ensure that there is a lawful basis for processing personal data and/or specific consent has been given for the data to be processed. This is important as the rights of individuals may be modified depending on whether the basis for processing their information is based on lawful processing or is based on consent. There are also requirements on organisations to ensure that privacy notices – the statements that are common on forms and documents where data is being collected – make clear what the lawful basis for processing data is.

In terms of consent, this must be 'freely given, specific, informed and unambiguous'[1] and there must be a positive 'opt-in', with a simple means for individuals to withdraw consent. The Information Commissioner's Office advises that 'individuals generally have more rights where you rely on consent to process their data'.

For individuals, GDPR gives the following rights[2]:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure (sometimes referred to as 'the right to be forgotten');
- the right to restrict processing;
- the right to data portability;
- the right to object; and
- the right not to be subject to automated decision making including profiling.

Within the concept of 'privacy by design', which GDPR gives a legal footing the expectation will be that data is held and processed at the minimum level required to fulfil an organisations functions and will not be held 'just in case', with only those with an explicit need to access the data able to access it.

[1] https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf
[2] https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf

GDPR also makes notification of a breach of data protection mandatory where this is likely to result in a risk for the rights and freedoms of individuals, with such breaches notified to the relevant supervising authority within 72 hours of an organisation becoming aware of the breach

GDPR also makes it mandatory for certain organisations to appoint a designated Data Protection Officer. The DPO must be sufficiently independent of the employing organisation and must have expert knowledge of data protection legislation.

Implications for the Board

Under its remit for effective College governance, the Board have a clear responsibility to ensure that arrangements for GDPR compliance are appropriate and meet the requirements of the legislation. This applies both to their responsibilities for New College Lanarkshire and for South Lanarkshire College, as both colleges will be subject to the new regulations.

Additionally, through the Secretary to the Board and appropriate professional advice, the Board will need to make sure that its own approach to handling, storing, processing, sharing and destroying personal data is GDPR compliant. This may require inclusion of specific GDPR / data protection input for new board members at induction and ensuring periodic refresher training is available for existing board members.

GDPR v UK Data Protection Law

The UK Government announced a Data Protection Bill in the 2017 Queen's Speech. This is expected to implement the GDPR standards across general data processing and provide any required clarity on definitions within GDPR in the UK context. It is also expected to contain specific provisions in relation to law enforcement, national security and, recognising the role of the UK Information Commissioner to update regulation and enforcement provisions in line with GDPR requirements.

However, where there is a difference between GDPR and any revised UK Data Protection Act, the College will still be required to maintain whichever standard is higher in relation to the personal data of EU citizens. In reality, this means that we must design all systems and processes to be fully GDPR compliant.

Resource Implications

GDPR will require the College to review all of our data protection arrangements in terms of the gathering, processing, sharing and destruction of data. In particular, this require a documented approach to recording explicit consent from the individual data subject(s) or the legal basis under which information is processed. Between now and May 2018, the College will be undertaking Information Asset Audits for each area of the College to ensure that we understand what data is held, why it is held, who it shared with and how/when it is destroyed.

An important aspect of the audit process will be to ensure that up-to-date and appropriate data sharing arrangements and agreements are in place, even where these may have been in place for some time. This will cover sharing of data with awarding bodies and any other external agencies with whom we are required to share information.

Much of this activity will be undertaken by the relevant managers and teams within the College, although in the initial stages, a working group will be a key driver in ensuring that appropriate processes are developed and

implemented across the College. However, it is clear that there will be an ongoing requirement to ensure that processes are relevant and effective and that these procedures are being adhered to.

Given the requirement that an organisations nominated Data Protection Officer must be sufficiently independent and free from any conflicts of interest, there is an additional resource requirement that will be needed to fulfil this role in the spirit of the legislation. In addition, given the changes to be introduced by GDPR and the implications of getting it wrong, it is important that the College ensures that our nominated DPO has sufficient expertise to fulfil this role effectively.

While it is possible that a DPO could be appointed from within an organisation and could undertake additional unrelated duties, the data controller or data processor 'shall ensure that such tasks and duties do not result in a conflict of interest' (GDPR, Art.39). There is also a requirement that the DPO 'shall directly report the highest management level of the controller or the processor' (GDPR, Art.38). It would be difficult to appoint an internal DPO at a level to report to the highest level of management who would not have other responsibilities, or who could be sufficiently independent in that they were not themselves involved in the processing of data for the organisation. In practice, this is what we have now.

To address this conflict in a cost effective manner while fully meeting our obligations, the College is currently part of a group of educational institutions exploring the possibility of developing a shared service via APUC (Advanced Procurement for Universities and Colleges) and UCSS (Universities and Colleges Shared Services). These discussions are at an early stage, but assuming that the service is implemented, this would enable New College Lanarkshire and South Lanarkshire to call down specific support to fulfil the requirements of the Data Protection Officer at a level appropriate to our needs. Costs of this service are currently being developed.

Subject Access Requests

As now, individuals will be able to make a subject access request (SAR) in relation to the information held about them by an organisation. However, one of the changes to the SAR process is that GDPR shortens the timescale for responses to a month, rather than the current 40 days under the Data Protection Act 1998. This is significant as, although the College does not receive a high level of SARs, they can be extensive depending on the information being sought. However, the need to strengthen recording and consent processes may assist in identifying where in the organisation information on an individual may be held.

Risk Management

Under current UK Data Protection legislation, the maximum fine for non-compliance or a significant breach is £500,000. However, this is much higher under GDPR, where the fine structure could be a fine of up to €20M or 4% of annual worldwide turnover, whichever is greater.

While this level of fine would be for the 'most serious' infringements, a tiered approach will apply and organisations could still be fined 2% of global turnover for failing to have its records in order, failing to notify the appropriate 'supervising authority' and data subject(s) about a breach or not conducting an impact assessment.

Our internal audit from January 2017 concluded that the College's data protection arrangements were 'Substantial'; however, due to the much greater implications of failing to have arrangements in place by May 2018 to comply with GDPR, a specific risk has been proposed for inclusion on the Regional Risk Management Register, to ensure independent oversight and regular monitoring of progress towards compliance.

Freedom of Information (Scotland) Act 2002

The requirements of GDPR do not alter the College's obligations as a named public authority under FOISA and do not change either the legal structure of enforcement or compliance arrangements. However, depending on the UK Government's approach to revising the UK Data Protection Act 1998, some review of cross referencing may be required.

Brian Gilchrist
Assistant Principal: Organisational Development
November 2017