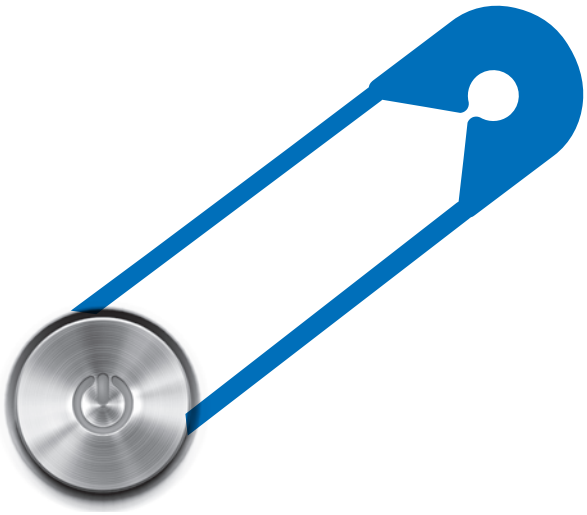
EVERSHEDS SUTHERLAND

Safety measures
GDPR obligations on Educational Bodies



The General Data Protection Regulation EU 2016/679 (the "**GDPR**") is effective on each member state from 25 May 2018 and will replace the Data Protection Acts 1988 and 2003 (as amended). In Ireland, the GDPR will be implemented by the Data Protection Bill 2017 (**the "Bill**").

It is envisaged that the GDPR will ultimately strengthen personal security rights relating to the storage of personal data. This enhanced protection, however, places a compelling duty on data controllers, such as educational bodies, to demonstrate how they have complied with the GDPR to ensure the rights of its data subjects are adequately safeguarded. The Board of Management/ the Education and Training Board will remain the data controllers for schools for the purposes of the Bill. Universities and Institutes of Technology will also remain data controllers under the Bill.

Consent and Processing Children's Data

A key change introduced by the GDPR is the higher bar set for relying on consent as a legal justification for processing personal information. The educational body must demonstrate that consent was freely given, specific, informed and unambiguous. All existing consents are required to meet this updated standard.

Under the GDPR, the digital age of consent refers to the age at which an individual is no longer considered a minor and may sign up for online services without parental approval. Under the current draft of the Bill, this has been adjusted to 13 years old. As such, parental consent will be necessary to process a child's data where the child is below the age of 13 years old. The data controller must endeavour to make reasonable efforts to ensure that the child is over 13 years old, taking into account available technology. It is not clear at this point whether this age of consent will apply to data subject access requests. Also, as per Section 9 of the Education Act 1998, parents of a student are entitled to have access to a school's records of that student's educational progress.

Data Access Requests

Under the GDPR, data subject access requests:

- require the provision of specific additional information to data subjects
- will not be subject to a fee unless the cost can be demonstrated as excessive
- must be processed within one month (as opposed to 40 days)
- can be restricted through national legislation when it is considered necessary for the protection of the data subject or to safeguard objectives of general public interest

A data subject access request may be refused on the basis that the request is manifestly unfounded or excessive, ie of repetitive character. National derogations may be introduced to further restrict the right of access.

Remedies/Sanctions

The significant increase in sanctions introduced by the GDPR are said to act as the primary deterrent against breaches of data protection rules. The level of potential sanction will depend on the breach. These include as follows:

- **Individual claims:** Data subjects can now sue both data controllers and data processors for compensation for non-pecuniary damage (e.g. damages for distress) suffered as a result of a breach of the GDPR
- **Administrative fines:** Fines can reach up to 4% of an organisation's annual worldwide turnover or up to €20 million

According to the current draft of the Bill, public bodies that do not qualify as undertakings[1] will not be subject to administrative fines and each activity will need to be evaluated on a case by case basis when determining whether to impose an administrative fine.[2] The Bill, as it stands, does not define a public body, however, other legislation has included various educational bodies within the definition. Until a final definition is provided in this context, it is suggested that each body identifies the performance of any private activities that may ultimately result in the body falling within the definition of an undertaking.

Personal Privacy Rights & Privacy Notices

The GDPR has resulted in enhanced control measures in favour of data subjects. This specifically introduces two new personal privacy rights, the right to (i) object to direct marketing, and (ii) data portability.

The former amends the status quo when an organisation is seeking information so that the data subject must "opt-in" where he/she wishes to receive information from the organisation. The latter refers to the data subject's ability to obtain and reuse his/her personal data for his/her own purpose.

Breach Notifications & Data Protection Impact Assessments ("DPIA")

Under the GDPR, where data processing "is likely to result in a high risk to the rights and freedoms of natural persons," data controllers are mandated to report a personal data breach to the Data Protection Commission (the "DPC") within 72 hours.[3] Data subjects will be notified where the breach is likely to result in a "high risk" to their rights.

Similarly, the implementation of a DPIA is mandatory where there is a high risk to individuals rights. The Data Protection Commissioner has described the DPIA as an important tool for negating risk, and for demonstrating compliance with the GDPR. While the DPC has not yet published a list of high risk areas, the Article 29 Working Party has outlined a list of criteria that is useful in assessing whether a DPIA is required. This includes the following:

1. Systematic monitoring: for example CCTV monitoring
2. Sensitive data: for example personal data relating to criminal convictions or offences which would be contained on vetting disclosures
3. Data concerning vulnerable individuals[4]
4. Innovative use of data eg fingerprint recognition services

[1] Head 23 of the Bill refers to the definition of an undertaking as set out in Section 3 of the Competition Act 2002, which provides that an undertaking is "a person being an individual, a body corporate or an unincorporated body of persons engaged for gain in the production, supply or distribution of goods or the provision of a service"

[2] According to Head 23 of the Bill, Article 83(7) of the GDPR derogates flexibility in the case of public authorities/bodies and states that administrative fines may be imposed on a public authority or body in respect of an infringement arising from its activity as an undertaking

[3] Article 33 of the GDPR. Please note data processors will only be obliged to report breaches to data controllers

[4] Paragraph 75 of the GDPR specifically identifies children as "vulnerable natural persons"

The rule of thumb appears to be that where it is not clear whether a DPIA is mandated, carrying it out is good practice and a useful tool to assist with compliance.

Data Protection Officers (the "DPO")

There is now a requirement for data controllers/data processors to appoint a DPO if the organisation (i) is a public authority/body, (ii) has core activities that involve large scale processing of sensitive data or data relating to criminal convictions; or (iii) engages in large scale processing of sensitive personal data.

Conclusion

A key way to demonstrate compliance is to conduct a gap analysis in order to identify areas that fail to fully comply with the GDPR, the actions required for compliance and update your data protection policy accordingly.

The educational body will need to organise an inventory of data to determine how future data will be managed and more particularly, how it intends to minimise the processing of personal data that is not necessary.

Finally, data controllers should be minded to implement proper procedures for notifying the DPC and/or data subjects of any potential data breach.

Margaret Gorman
Partner & Head of Education

+353 1 6644325
margaretgorman
@eversheds-sutherland.ie

Marie McGinley
Partner, Head of IP, Technology & DP

+353 1 6441457
mariemcginley
@eversheds-sutherland.ie

Bernard Martin
Solicitor

+353 1 6644234
bernardmartin
@eversheds-sutherland.ie

Ciara Geraghty
Solicitor

+353 1 6644336
ciarageraghty
@eversheds-sutherland.ie

eversheds-sutherland.ie

EDUB.1532 12/17