DATA PROTECTION IN THE EDUCATION SECTOR: THE TRAINING CHALLENGE

Category: Privacy Law, Infosec, and POPIA,Technology Law
written by Delphine Daversin | February 8, 2019

Today's students will be the first generation with a digital footprint from birth. This can be seen as a major threat for them. At the same time, the diffusion of information technologies in education, conducted with discernment, is also a major transformation tool for their success.

It has to be noted that education remains an under-explored sector in terms of privacy and cybersecurity.

It is crucial that the personal data of all members of the educational community (students, parents, teachers and more generally personnel) be protected and processed in accordance with applicable laws.

It therefore seems essential to make these players aware of their duties and rights in terms of privacy.

Policy-makers and regulators should also play their part by:

- developing awareness of all actors of the educational community;
- promoting codes of conduct in the education sector; and
- supporting school institutions in their compliance programs with applicable privacy laws, by designing and spreading compliance toolkits.

The UK Information Commissioner's Office ("**ICO**") recently released a guideline entitled "*Data Protection: a toolkit for schools*" which gives valuable guidance and tips for educational institutions. The salient points of the 8-step plan proposed by the ICO are summarised below.

Step 1- Raising Awareness

Training and awareness should be as inclusive as possible.

It can be efficient to "*link data protection to safeguarding children (and child protection) when trying to get people engaged. In this way, all staff see that data protection matters in the context of pupil*

welfare".

In addition, it is important that "*the language associated with data protection, and the enhanced legislation, is demystified.*"

Step 2- Creating the school data ecosystem

The school should build up a high level data map and a data register, drawing an overview of the school's "data ecosystem".

This picture of the eco-system can then be "*discussed and tested with staff to identify any gaps in the initial 'overview' and build confidence that everything is captured*".

This picture of the data eco-system will also help communicate personal data use with pupils and parents.

Step 3- Documenting the reasons for processing data

Schools are collecting and hosting a fair amount of sensitive data about children, from their family background to their health conditions.

It is crucial for the personnel involved in data processing to "*understand the extra reasoning that is required to process special categories of data, which are tightly defined*" in applicable data protection laws.

It is also key to "*Identify the areas that do not appear to be essential to undertake the task of safely and efficiently running a school, as these are the areas that specific consent from data subjects may need to be sought if not already obtained*".

Step 4 – Documenting how long you need to retain information

The ICO advises to create a personal information retention policy that can be discussed and iterated with those who best understand your uses of data. The ICO reminds the simple rule of thumb: "*Understand that data retention is based on justification – if you can justify it, you can keep it*".

Step 5 – Reassurance and risks

The ICO suggest a three-step approach:

- identify risks that emerge from the initial completion of the data eco-system;
- assess what can be done to eliminate or reduce risks and set action plans; and
- use Data Protection Impact Assessments as a part of the risk identification and mitigation procedures.

Step 6 – Understanding and deciding on the appointment of an Information Officer or Data Protection Officer

Depending on the data protection laws the school is subject to, this appointment might be mandatory or not. Even in cases where this appointment is not mandatory, the role of the information officer is key in terms of spreading awareness and advocating for compliance within the organisation.

Step 7 – Communicate with data subjects

The educational institutions owe complete, fair and transparent information to all data subjects

regarding processing of their personal information. The ICO recommends to:

- be familiar with the full potential rights a data subject has, and the circumstances in which these do not all apply, that is to say exemptions exist;
- be able to demonstrate compliance with data protection laws, as compliance alone is not enough.
- liaise with their professional bodies and information regulator to get guidance on best practices in terms of privacy notices for communicating with parents and pupils;
- "*gain benefits from being open and transparent with data subjects, there is more to building trust than compliance alone*";

Step 8 – Operationalise Data Protection, and keep it living

Schools should identify the range of policies they require that cover the procedures and processes for data protection.

They should also have a good understanding of what a data breach is and have a clear procedure in place in case a breach occurs.

Finally, they should ensure that data protection and risk management is a core and regular part of decision-making and risk management practices within the school.

If you would like assistance in preparing your educational institution for data protection laws such as the Protection of Personal Information Act, 2013, please contact us.