The GDPR and Schools - One Year On … what we know

The ICO (Information Commissioners Office) revealed that there were 6,281 referrals from schools between the 25th May (when GDPR came into force) and the 3rd July 2018. This is a ***160% rise*** in complaints over the same period in 2017. Of those affected, ***71% downloaded malware*** and ***50% experience phishing attacks***, both of which exploit human error; ***data losses (82%)*** and ***remediation costs (47%)*** were the biggest concerns in relation to these attacks.

A survey of 156 schools and colleges across the UK has revealed that even though over a year has passed since GDPR was implemented in the country through the remodeled Data Protection Act, 52% of them are still not fully compliant with GDPR.

Only 48% of schools and colleges say they are GDPR compliant.

Despite such rigorous penalties being ensured by GDPR, over half of schools and colleges in the UK are still not fully compliant with GDPR even though a large majority of them are aware of the fact that monetary fines imposed under the new DPA would "significantly impact" them, a survey from Trend Micro and RM Education has revealed.

As noted by the TES, while 52% of UK schools and colleges have admitted to not being fully compliant with GDPR, 46% of them said that a lack of security awareness is preventing them from being fully compliant and another 39% said a lack of financial investment is the biggest factor behind their inability.

Considering that 79% of schools and colleges fear that monetary fines imposed under the new DPA would "significantly impact" them, it is clear that they are aware of what GDPR entails but a lack of resources and support is preventing them from accomplishing GDPR compliance.

However, while 19% of schools and colleges fear that cyber criminals could pose the biggest threat to them in the future, 75% of them believe that accidental loss of sensitive data by their staff could expose them to GDPR fines.

"Things as simple as leaving a memory stick lying around, not changing your password regularly, or not updating to the latest software could have a seriously big impact. Having a strategy in place to ensure all data is protected, and able to be deleted should a pupil or parent request it, is also key," said Bharat Mistry, principal security strategist at Trend Micro to TES.

As per GDPR, schools need to "ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services" and therefore, have to ensure that the systems they use are always updated with the latest security patches and that data is always encrypted or stored securely.

According to the UK's Action Fraud department, schools have already been targeted by hackers posing as the 'Department of Education' and trying to trick employees into clicking on links or installing ransomware which the hackers can then use to take control of systems and demand money.

… Continued Overleaf

Three Education / School Examples of Issues ...

School Management Systems
A bug in an information management system used by 21,000 UK schools almost resulted in a major data security incident after it was discovered that the software incorrectly matched contact details of students with their names.

Thanks to the bug, a student or the student's parents could view e-mail addresses, phone numbers, and physical addresses of other students once they were contacted by their schools using any of these methods of communication.

"The consequence of the corruption is that contact information for the incoming pupil for example, address, telephone number and email address, may have become associated with other pupil's records, or the new pupil could themselves be linked to the wrong contact details. The problem could have impacted pre-admissions, pupils on roll and the records of school leavers," said Capita, the developer of the information management system in an e-mail to schools.

A UK University
A UK university was fined £120,000 by the ICO for not managing data related to a project involving schools and teachers.

The university had led on an educational project involving schools, teachers and university staff in 2008/09. They communicated with everybody electronically, kept records of the schools progress and the finishing results. However, when the project finished they did not delete the data files, but kept them on a server.

The ICO stated that although the data was never used again, the fact that it had been kept put the details of individuals involved at risk and it should have been securely deleted a long time ago.

An International Perspective
A watchdog has penalised a local authority for trialling facial recognition on high-school students in Sweden to keep track of attendance.

The Swedish Data Protection Authority (DPA) fined the Skelleftea municipality 200,000 Swedish Krona (£16,800, $20,700) for flouting a privacy law. This is the first time that Sweden has ever issued a fine under GDPR. The trial involved tracking 22 students over three weeks and detecting when each pupil entered a classroom.

The General Data Protection Regulation, which came into force last year, classes facial images and other biometric information as being a special category of data, with added restrictions on its use. The DPA indicated that the fine would have been bigger had the trial been longer.

ur

The GDPR was not a singular event - it's impact and legal expectations will be with us for a long time. Schools have been - and are - vulnerable to it's reach. We have already advised over 100 schools and manage the data protection in over 20 others on an on-going basis.

Don't put your school at risk - Illuminate Learning can help your school become compliant. You can never remove all risks - but you can reduce the probability.

Contact us to book a place on one our courses, get individualised support or purchase one of our resources.
Visit : www.illuminatelearning.org or e-mail us on contact@illuminatelearning.org