How Does GDPR Affect the Education Sector in the Middle East?

Camelia Quinnell - Senior Data Protection Adviser - Digital & Data
- Dubai International Financial Centre

The General Data Protection Regulations ("GDPR") came into effect on 25 May 2018. The GDPR, which replaced the EU's Data Protection Directive of 1995, represents a significant expansion of personal privacy rights for EU residents.

The politically challenging task of escalating privacy protection from a directive to a binding regulation began in 2009 and involved protracted negotiations among the European Commission (the EU executive body) and its two legislative chambers, the Council of the European Union and the European Parliament. This was partially motivated by the desire for uniform protections for all EU residents and partially necessitated by the needs of regulated entities for consistent compliance requirements across the EU.

Why should Middle East institutions pay attention to GDPR?

It is widely known that the GDPR has more enforceable legal status in comparison to the previous Data Protection Directive, and it is also substantively more robust in a number of significant ways. The most notable of these for entities located in the Middle East is that, unlike the Data Protection Directive (which mandated compliance by entities with a physical EU presence, such as a processing center or even a server), the GDPR's coverage extends to entities with no physical EU footprint if they process personal data of EU data subjects residing in the EU. This limited extraterritoriality, while a significant expansion of the reach of EU law to entities outside the EU, does not attach to EU citizens abroad. As such, a Middle East entity involved in a data transaction with an EU resident in the Middle East, for instance, would not be subject to the GDPR; the same entity engaging in significant and intentional cyber-transactions with EU residents would be.

Why education providers should pay attention to the GDPR?

Middle East-based Education institutions newly affected by the extraterritorial reach of GDPR are those that target distance education programmes to EU residents who are physically located in one of the member states. Such programmes were not initially subject to EU privacy law under the Data Protection Directive if they did not have infrastructure within the EU, but are now covered under the GDPR, even if they have no physical presence within the EU. However, Article 3 of the GDPR suggests that incidental transactions, such as the mere availability of goods or services via a website, are not automatic grounds for subjecting non-EU entities to the GDPR.

On the face of it, it is tempting to believe that Education institutions that enrol EU residents in the Middle East are entirely exempt from compliance with the GDPR. This would certainly be true for EU residents who initiate their admission application process from outside the EU. In the case where EU applicants start the admissions process from their home countries and obtain visas to enter the Middle East after gaining admission to eligible programmes, the GDPR will apply and such institutions would need to demonstrate compliance. In essence, active student recruitment campaigns targeting EU residents could subject the data collected from such students, whether via automated or non-automated means, to compliance requirements under the GDPR. It may take a few years for a more precise understanding of how the GDPR will be further defined, interpreted, and enforced by the EU and national data protection authorities of its member states. At such early stage, it is probably unlikely that the most expansive interpretation of the regulation's extraterritorial application would be immediately enforced against non-EU entities. It is clear however that institutions with significant engagement with the EU, either in the form of physical presence or of distance-delivered services, should take immediate steps to ensure compliance with the GDPR.

Whose data does GDPR protect?

Personal data of all living individuals physically within the EU ("EU data subjects") are covered by the GDPR. The regulation makes no distinctions based on individual's permanent places of residence or nationality. The GDPR applies to all such individual's personal data, defined as any information that can be used to, directly or indirectly, identify a person. These include not only such obvious information as educational, financial, employment-related, and health data, but also photographs, personal phone numbers, and IP addresses.

How should the education sector prepare for GDPR?

Education providers in the Middle East should consider a number of action points as part of their GDPR compliance preparations as follows:

Data Review: A comprehensive review should be undertaken to determine (i) what personal data is currently held, (ii) how that data was acquired, and (iii) for what purpose it was acquired. Education providers should consider whether they have obtained and hold such personal data in accordance with the requirements of GDPR. If they have not, such data should be deleted, or consideration should be given as to how its continued storage / use may be rendered GDPR-compliant.

Privacy policies: privacy policies are a key element of the new regime. Education providers should review their existing privacy policies, and make all amendments necessary to bring them into line with the GDPR's requirements.

Consent: this is unlikely to be the most appropriate lawful basis for the processing of personal data by Education providers going forward. The GDPR requires that consent must be able to be withdrawn as easily as it is given and processing must immediately stop. Clearly, this is not practical given Education providers' obligations to protect the safety and welfare of their students. Education establishments will need to look to other bases provided in the GDPR to ensure that their processing activities are lawful. This is a more complex legal question, and will be based on a case-by-case basis, the operation of the education provider in relation to the data.

Consent must be given for the processing or flow of personal data to third-parties, so in order to become GDPR compliant, education providers must be aware of where various pieces of data are going and why.

Data Security and Third-Party Agreements: a comprehensive, written information security programme should be developed and implemented to protect the security, confidentiality and integrity of personal data held. A review of arrangements with all third-parties engaged to handle, store or otherwise process personal data collected and/or stored by the institution should be undertaken. The GDPR requires all data controllers to have binding contracts with the parties that process data on their behalf. For education providers, it is important that all current service level agreements and other contracts with third-party suppliers are carefully reviewed and amended to ensure they are GDPR-compliant.

Supervisory authorities and penalties

Under the GDPR, EU member states have to designate qualified supervisory authorities with specified oversight, investigatory, and enforcement powers to implement its requirements . These authorities will oversee compliance, provide consultation and prior approvals, and receive and administratively adjudicate complaints against controllers and processors. They can also impose fines of up to two percent of the global revenues for certain penalties, and up to four percent of such revenues for more serious ones.

Just as important as the supervisory authorities' power to impose penalties is the consultative role they are assigned in reviewing mandatory data protection impact assessments that data controllers and processors must regularly perform in connection with high-risk processing activities prior to implementing them.

Conclusion

The GDPR took years to be adopted, and it may be safe to assume that it will take years before its real

impact and practical compliance requirements become fully settled.

Education providers in the Middle East with EU-based operations and those with significant numbers of EU residents as students — particularly those delivering distance education programmes to such students within the EU — should start to map out a strategy of implementing GDPR-compliant practices now.