THE NEW ERA OF EDUCATION: HOW CAN EDUCATION PROVIDERS REALISE THE POTENTIAL OF EDTECH WHILST PROMOTING PRIVACY AND SECURITY?

Gemserv

2

Education technology, also known as EdTech, involves the use of technological resources to support teaching and the daily administration of education in the classroom at schools and universities. EdTech includes a broad category of products, tools and apps that aim to enhance pedagogy.

According to a global educational census carried out by Cambridge International[1], there is a rise in implementing technology, in conjunction with traditional learning methods, to improve education. This conclusion is based on an online survey of nearly 20,000 teachers and students (aged 12-19) from over 100 countries. As per the report, the figures clearly show that new technologies are rapidly becoming embedded in the modern era of education globally, supplementing traditional tools such as blackboards and whiteboards with use of desktops, smartphones and tablets.

In England, the Department for Education published a strategy policy paper[2] in April 2019 which aims to promote the development and embedding of high-quality EdTech. The key areas of opportunities for EdTech to make a difference have been identified as follows:

- Improvement of 'non-teaching' administration processes
- Assessment processes
- Effectiveness of teaching practices and student performance
- Continuous professional development of educators

Education providers must therefore be better equipped to adopt EdTech and engage with EdTech businesses that can meet the needs of the users and promote the good use of technology.

The key growing concerns around the use of EdTech relate to the access, and the use of, student personal data created and gathered by educational apps, websites and other online services.

SO, WHAT ARE THE KEY POINTS TO CONSIDER FROM A PRIVACY PERSPECTIVE?

PROCESSING CHILDREN'S DATA

Where students are children, as per the Recital 38[3] of the General Data Protection Regulation (GDPR), they "(...) merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. ... In particular, [where] the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child."

The GDPR categorises children as "vulnerable natural persons". The lawful processing of children's data is specifically addressed in Article 8[4] of the GDPR, irrespective of lawful processing under Article 6[5]. Article 8 of the GDPR only applies to "information society services" that offer services directly to a child under the age of 16.

It states that "(...) where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child." Parental (or guardian) consent is required for all information society services that collect children's data, regardless of whether or not they have a lawful basis for processing the data.

Individual member states of European Union may lower the age, but not below 13 years old. Information society services include "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services". By this definition, EdTech is in scope.

Article 8(2)[6] puts the onus on the controller "(...) to make the reasonable efforts to verify consent". This would essentially mean that the education provider and the EdTech organisation must first carefully work out the nature of their business relationship to understand their respective obligations under the GDPR.

Also, ways to obtain consent in the child's context has not been defined under the GDPR, therefore the controller must follow and implement Article 7[7] conditions for consent.

1 https://www.cambridgeinternational.org/Images/514611-global-education-census-survey-report.pdf

2 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/791931/DfE-Education_Technology_Strategy.pdf

3 https://gdpr-info.eu/recitals/no-38/

4 https://gdpr-info.eu/art-8-gdpr/

5 https://gdpr-info.eu/art-6-gdpr/

6 https://gdpr-info.eu/art-8-gdpr/

7 https://gdpr-info.eu/art-7-gdpr/

3

When processing children's personal data, the GDPR imposes further requirements under Recital 58 which states that "(...) Given children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand." This translates into a requirement to communicate clearly and in a plain manner to children.

PRIVACY AND SECURITY BY DESIGN

Whilst education is inevitably changing, the concerns around breaches of privacy, security and safety remain a barrier to adopt new technology in the education sector. To mitigate any potential risks, before deploying a technology, education providers are directly responsiblefor ensuring that the technology solution provides an appropriate level of security measure to safeguard data. Education providers must proactively adopt a privacy by design and default control framework to audit risks, overcome any post-deployment privacy gaps and comply with Article 25[8] of the GDPR.

An adequate privacy by design and default control framework must achieve the following:

1. It must identify the need to carry out a Data Protection Impact Assessment to assess the impact of new technology
2. It must assess whether privacy and security are embedded in the design of the EdTech by reviewing aspects such as, user authentication, access control, encryption of information, etc
3. The management of breaches by the implementation of a breach management process, especially when more than one organisation is involved in the processing of data
4. The implementation of training for personnel who have access to personal and confidential information
5. The protection of personal data by third parties by implementing agreements governing issues such as cross-border transfer, use of personal data and cooperation requirements, as well as the controls that third parties have implemented to meet the terms of the agreement
6. The transparency of privacy policies, and practices to ensure that technology is user-centric

AGE APPROPRIATE DESIGN

Furthermore, the UK's Information Commissioner's Office (ICO) reccently released the final Age Appropriate Design Code of Practice. It sets out 15 standards of "age appropriate design" (on data sharing, geolocation tracking, profiling, etc.), which online service providers such as EdTech providers must comply with when designing online services that children under the age of 18 are likely to access. The standards are based on data protection law principles and are legally enforceable under the GDPR and UK Data Protection Act 2018.

The Secretary of State will now need to lay the code before Parliament for its approval as soon as possible. As per the ICO's statement, organisations will have 12 months to implement the necessary changes from the date that the code takes effect following the Parliamentary approval process.

Education providers must verify that EdTech providers have policies and procedures in place that demonstrate how EdTech companies, as a provider of digital services, comply with their data protection obligations and the Code.

8 https://gdpr-info.eu/art-25-gdpr/

LONDON OFFICE

8 Fenchurch Place

London, EC3M 4AJ

Telephone: +44 (0)20 7090 1091

dataprotection@gemserv.com

IRELAND OFFICE

Fitzwilliam Hall Business Centre

Fitzwilliam Place, Dublin 2

Telephone: +353 (0) 1 669 4630

bd@gemserv.com

Gemserv