The impact of GDPR on education

Petra Wildemann
21 May 2018

Anyone who imagines that the impact of GDPR, which will take effect as of May 25th 2018, will be mostly limited to large corporations, should consider the field of education, where students, teachers and parents interact with large quantities of highly sensitive data.

Data protection in the field of education has become a difficult topic since Web 2.0 applications started to play a role in communication. The development of Web 2.0 applications includes the active and interactive use of the internet, in particular with respect to dynamic websites, known as SNS (Social Networking Sites). A phenomenon first seen as a tool to support teachers engaging in modern communication has now become a thorny data protection issue. Information on paper can be physically destroyed, but electronic data often cannot really be erased. It remains in systems even after we think we've deleted it. We have in fact little or no control of the information we publicize so casually in social networks.

The proper use of social media poses a greater challenge for schools than for businesses. You may wonder why this is so. Consider: in the school environment, we have business people (parents), who are using social media such as LinkedIn, Xing or others. You seldom find kids on those platforms. They are using Instagram, Facebook or Pinterest and casually posting pictures of themselves with little thought to how these pictures might hinder them later on when they start their careers. Ideally, teachers should know all about all of these platforms in order to advise students on how to use them properly.

Sensitive data, in particular involving children and young adults, has to be protected. Therefore a Data Protection Officer is highly recommended for all businesses which deal with sensitive data with a potential for misuse. This is an eventuality which few foresaw when the social media communication platforms were established. Data Protection needs to be attended to whenever interactive internet services are used.

But what is personal data? Does everything that has anything to do with a person count as personal data? Some data is clearly personal, but there can be grey areas. But it is clear that some data transmitted by students as well as teachers fits in this category, and therefore are a cause for worry, especially when SNS are used for the transmission. SNS is not only a platform for communication; it has become over time a trade-business: "You use my portal and I use your data". The value of SNS services has a very high market capitalization. In addition, SNS firms are under enormous pressure to grow their business. „Friendship" in the social networks has an increasingly quantitative aspect. Often information is shared which most people would never dream of revealing face-to-face. And therein lies the basis for fraud, cybermobbing, cyberstalking, cyberbullying and many other new ways to harm people by improperly using the information they have casually revealed. The internet doesn't understand intimacy and that is where users of social networks are getting it wrong.

The impact of GDPR on education

We are all part of the transmission of personal information. Many people casually reveal information about their personal lives just to obtain attention. Newsletters, surveys, quizzes/competitions, reward cards and travel information are some of the key data collection methods where people are least on their guard and casually reveal a dangerous amount of personal information about themselves. The internet has no "loss of memory". What has been published can very seldom be deleted or destroyed.

The field of education has an important role to play in the use of SNS. You will not succeed in forbidding people to use such portals. Therefore, school administrators should provide services in the form of data protection guidance for the students, parents and teachers. The better all of them are informed, and use the same processes to protect their own data, their colleagues's data and their students' private data, the less the likelihood that data leaks and misuse of personal data will become an issue with colleagues, students and parents.

Where risks are involved, there is protection through insurers. What happens if the right level of data protection is not included in processes where sensitive data can be transferred from one entity to another? Is this a topic which the insurance industry should pay more attention to?

[Data Protection in the education business - educa.ch](#)

Further information:

European Network and Information Security Agency ENISA. Position Paper No. 1: Security Issues and Recommendations for Online Social Networks (PDF).
Editor: Giles Hogben, October 2007.

Bericht und Empfehlung zum Datenschutz in sozialen Netzwerkdiensten «Rom Memorandum», März 2008 (PDF)