PROTECTION OF PERSONAL DATA IN E-LEARNING - METHODOLOGY AND TECHNOLOGIES

Svetlana Toncheva-Pencheva[1], Yordanka Anastasova[2]

[1] University of Mining and Geology "St. Ivan Rilski", 1700 Sofia, svetlana.toncheva@mgu.bg
[2] University of Mining and Geology "St. Ivan Rilski", 1700 Sofia, yordanka.anastasova@mgu.bg

ABSTRACT. Personal data protection and privacy are a key focus in the work of all institutions that deal with them. The implementation of Regulation 2016/679 of the European Parliament and of the Council of Europe of May 2018 requires that this protection also applies to all types of information systems. In this respect, the introduction of technologies and the establishment of a methodology for e-learning systems, which are increasingly being used by educational institutions, are indispensable. The article discusses possible technological mechanisms for personal data protection and offers a methodology to be implemented in an e-learning system. The proposed methodology is basic and includes fundamental rules for the protection of personal data. Depending on the type and purpose of the specific e-learning system, it can be complemented and further developed.

Key words: e-learning, personal data protection, technologies, methodology

ЗАЩИТА НА ЛИЧНИТЕ ДАННИ ПРИ ЕЛЕКТРОННО ОБУЧЕНИЕ – МЕТОДОЛОГИЯ И ТЕХНОЛОГИИ

Светлана Тончева-Пенчева[1], Йорданка Анастасова[2]

[1] Минно-геоложки университет „Св. Иван Рилски", 1700 София, svetlana.toncheva@mgu.bg
[2] Минно-геоложки университет „Св. Иван Рилски", 1700 София, yordanka.anastasova@mgu.bg

РЕЗЮМЕ. Защитата и неприкосновеността на личните данни се налагат като основен акцент в работата на всички институции, които боравят с такива. Прилагането на Регламент 2016/679 на Европейския парламент и на Съвета на Европа от май 2018 г. изисква тази защита да се приложи и към всички видове информационни системи. В тази връзка е задължително въвеждането на технологии и създаване на методология и при системите за електронното обучение, което навлиза все повече в образователните институции. Статията разглежда възможни технологични механизми за защита на личните данни и предлага методология, която да бъде реализирана в система за електронно обучение. Предлаганата методология е базова, като в нея са включени основни правила за защита на личните данни. В зависимост от вида и предназначението на конкретната система за електронно обучение може да се допълва и доразвива.

Ключови думи: електронно обучение защита лични данни, технологии, методология

Introduction

The main characteristic of modern economy is the need to acquire knowledge, skills and qualifications throughout life. The massive use of information technology for training needs necessitates the use of principles that best protect the personal data of each learner.

The changes introduced by the General Data Protection Regulation (GDPR) require the introduction and enforcement of privacy and privacy rules. In this respect, the introduction of technologies and the establishment of a methodology to ensure the highest degree of protection of all personal data used in training are necessary.

Cases of cybercrime related to theft or misuse of personal data have led to the introduction of privacy technologies.

The basic legal principles on which the lawful use of personal data is based in Bulgaria are set out in the Personal Data Protection Act, which has been in force since 2002.

Security and education

Higher education has gradually started to introduce technology and information systems for e-learning to meet the wishes of students who want something beyond traditional teaching methods. These new training technologies mix online computerized content for a course with various blogs, forums and Webinars.

In this training, students want to use increasingly new tablet and mobile applications that may endanger the security of the e-learning platform used by the university.

Students are one of the largest groups of users of various social networks such as Facebook, Twitter, YouTube and others, seeking to reconcile their use with e-learning platforms. This facilitates the distribution of malware, which may also be related to the theft of personal data from university servers.

For this reason, it is of particular importance to introduce a methodology for working with the e-learning platform of the particular university, which will maximally protect both the

personal data of all learners and the technologies that protect the e-learning system itself.

Personal data protection technologies for e-learning systems

Generally, e-learning systems use the Internet as the main channel for information transfer, trying to prevent attacks on all student communication with the training system. In order for this to be achieved, it is necessary to introduce technologies that, in their joint work, ensure maximum protection of the system and personal data.

A basic technological requirement is to ensure the confidentiality of the network through which data is transferred. Relatively good data security is provided by technologies, such as secure sockets layer and virtual private networks, but they are not entirely sufficient. Since students are using different learning devices, it is necessary to provide protection for all possible channels of communication.

In this connection, the eLearning system may require the use of an additional technology requirement, such as registration of the location and the devices used by each student. The eLearning system can require anyone to register in their individual profile the location and all the devices they use to get learning content, and to impose limitations on the number and type of devices used. It is possible to introduce limitations on the IP addresses used by the trainee in e-learning and distance learning systems that provide specific learning content. A requirement may also be that tests are to be performed only from fixed fixed-term addresses and in specialized centers.

Another additional technology requirement is the site that accesses the e-learning system to use the P3P developed by the World Wide Web consortium. Through this technology, students can easily be informed about the rules on personal data in the system. This technology provides a mechanism that ensures that users are informed about privacy policies before submitting personal information but does not provide a sufficiently reliable mechanism to ensure that the site is working in compliance with this policy.

A technology solution used is an Anonymizer web service to redirect web queries. Combined with secure communication channels, this approach may be well suited to protecting information in e-learning systems. Even better protection would occur if this proxy server is configured on a virtual machine, which will provide an extra level of data protection.

There are also other defense technology solutions such as Onion Routing (D.Goldschlag, M.Reed, P.Syverson, 1999), Crowd (Reiter, MK, A.D.Rubin, 1998), MIX Networks (D. Chaum, Net (D. Chaum, 1988) and others, but in addition to good personal data protection, they can cause some inconvenience in handling them, some of them commercial.

Perhaps the best technological solution is to implement cryptographic functions and use a fully encrypted connection when transmitting the information, but this will further burden the e-learning systems.

In order to assess what combination of technologies will be applied to each specific e-learning system; a preliminary analysis is needed to determine the balance between the protection of personal data and the quality and speed of the information exchanged.

Methodology for the protection of personal data in e-learning systems

The methodology for personal data protection can include a number of rules that need to be laid down in the process of designing and implementing the e-learning system concerned. These rules and requirements are directed both towards the users of the training system and towards the persons involved in the administration of the system.

Depending on the objectives of the e-learning system, the proposed electronic content and the validity of the certificates issued, the methodology may include a different set of rules, but the basic data protection standards are:

- Defining user groups in the system;
- Defined mechanism for registration, entry and exit of the system;
- Accountability;
- Term of storage/erasure of personal data and information;
- Rules for the transfer of personal data to other authorized institutions.

Defining user groups

Already in the process of designing the e-learning information system, it is essential to define the main user groups, such as the administrators of the system itself, the training administrators, leading lecturers for each course and some systems and users with special powers.

From the point of view of personal data protection for each user group in the particular system implementation, the "minimum sufficient amount of information" rule is used. For each group of users, the system only provides access to the information required for their specific work. Thus, the e-learning system designs rules for personal data protection.

To accomplish this, a detailed description of the entire amount of information that will be exchanged during the actual operation of the system is necessary.

A defined mechanism for registration, input and output

Obligatory conditions in the methodology are strict compliance with the mechanisms for registration of users, entry and exit of the system.

Depending on the requirements of the specific e-learning system, the type of information exchanged and the platform used for its implementation, input/output mechanisms are introduced and controlled. It is imperative to use an account that includes at least a unique user name and password that

are obtained by filling in all the fields in the registration form of the system. For some systems, the password is set by the system and is not subject to change, while others require additional activation by code, e-mail, etc. after verification of the information entered by the user.

If the training system includes financial instruments, the so-called "fiduciary mechanisms" are introduced that include the use of encryption and various types of digital certificates that the system generates.

In this additional security mechanism, you can also define the number of account entries, authorization time, device verification, single key session encryption, automatic shutdown, and system shutdown in case of suspected attack and other security mechanisms.

Accountability

Accountability in e-learning systems is directly related to the control of input and output mechanisms used.

Logs for all system events such as login, exit, session duration, user authorization, access to system resources, duration and time of use, passwords used and other defined requirements are required.

Systematic reporting mechanisms check these logs - periodically or continuously - and in the event of inconsistency or suspicious action they end or block the work of the user concerned.

Term for storage/erasure of personal data

In the implementation of the e-learning systems, rules on the term of storage of personal data are defined, which must correspond to those stipulated in the legislative acts of the government.

The storage methodology sets both technological and organizational measures for archiving and long-term storage outside the system, subject only to regulatory mechanisms for the protection of personal data.

An important element is the permanent deletion of personal data, and it should be possible for them to be deleted at the request of the person concerned, if this is not in contradiction with the normative acts.

Rules for the transfer of personal data to authorized institutions

Many e-learning systems that are associated with issuing different types of certificates require the transmission or sharing of personal data to users.

Already at the design stage of e-learning systems, strict rules are laid down which set out a legal framework for the exchange of personal information between the educational institution and the relevant governmental institutions. The mode of transmission, the type of data and the authorized personnel to do this are specified.

The training on the protection of personal data both by the administrators of the system in the university and the users of this system is also an important part of the methodology.

Conclusion

E-learning today is an integral part of higher education, with more and more universities taking advantage of the benefits it offers when it comes to further qualification or retraining.

The rules imposed by Regulation 2016/679 on the protection of personal data of the European Parliament and of the Council of Europe require the introduction of technological solutions and mechanisms in the systems used that fully comply with those rules.

To respond to these challenges, it is imperative to add new functionalities to existing eLearning systems. When creating new ones, it is imperative to apply a methodology that includes different technological mechanisms to ensure the protection of personal data.

It is important to make sure that as personal data protection technologies evolve, development is also subject to attempts to modify or steal them, and therefore data security methodology and technologies need to be complementary and further developed.

Depending on the information contained in the e-learning system, the most appropriate mechanisms according to the development are applied. However this must not hamper the basic functionality, namely the provision of electronic content to authorized users.

References

Закон за защита на личните данни (Zakon za zashtita na lichnite danni), https://moew.government.bg/static/media/ups/articles/attachments/ZZLD8acf0a6196912da30c4353f7d9e77f39.pdf, May, 2018.

Anonymizer web service at: http://www.anonymizer.com/, April, 2018.

Chaum, D., "Untraceable Electronic Mail, Return Address, and Digital Pseudonyms", Communications of the ACM, vol.24 no.2, 1981, p. 84-88.

Chaum, D., "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability", Journal of Cryptology 1/1 ,1988, p. 65-75.

Goldschlag, D., M.Reed and P.Syverson, "Onion Routing for Anonymous and Private Internet Connections", Communication of the ACM, vol.42, no.2, 1999, p. 39-41.

Reiter, M.K. and A.D.Rubin, "Crowds: Anonymity for Web Transactions", ACM Transactions on Information and System Security, v. 1, n. 1, 1998, p. 66-92.

http://www.w3c.org/P3P, April, 2018.