2022 15th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI) | 978-1-6654-8887-7/22/$31.00 ©2022 IEEE | DOI: 10.1109/CISP-BMEI56279.2022.9980175

Data Privacy Protection from the Perspective of GDPR - A Case Study on E-learning Platform "SHCneo"

M.A. Jiayi Chen
University of Shanghai for Science and Technology
Shanghai, P.R. China

Dr. Jingwei Xu*
University of Shanghai for Science and Technology
Shanghai, P.R. China
*Corresponding Author

Abstract—**In order to avoid the risk of privacy leakage during using E-Learning platforms, E-Learning Platform "SHCneo" - jointly built by Chinese and German universities follows the most strict General Data Protection Regulation (GDPR) in EU for protecting the personal privacy of teachers and students. Based on the introduction of current network security development on E-Learning platforms in China and other countries, we use SHCneo as a case study, analyze the characteristics of GDPR's personal data privacy protection, try to explore the improvement of the data privacy security in online learning system, and summarize a few data privacy protection measures.**

Keywords- GDPR; data privacy protection; SHCneo

I. INTRODUCTION

The COVID-19 pandemic has brought unprecedented challenges to our safety, health and education. According to the report in August 2020 by UNESCO, there are approximately 1.5 billion students all over the world, of which 1 billion – two-thirds of the students – are facing the uncertainty school closures. Of the 900 million students starting the new school year, more than half of them are expected to study entirely remotely, or for some of them, have to study completely online or with blended learning[1]. A report from UNESCO on July 13, 2021 "What's Next? Lessons on Education Recovery " [2] also mentioned, more effective distance learning systems are better able to withstand future crises and benefit all students [3]. In this special situation, many students have to study online. Along with a large amount of personal data being shared, the security risk of personal data is also exposed. UNESCO has also listed personal data and privacy protection as one of the great challenges during distance education. How to protect personal data and privacy in online learning platforms has become an important issue faced by students, teachers and parents.

II. THE CURRENT SITUATION OF NETWORK SECURITY DEVELOPMENT OF TEACHING PLATFORMS AT HOME AND ABROAD

With the development of information technology and the popularization of the Internet, more and more countries and organizations have formulated laws, regulations and policy documents related to personal data protection, and adopted various measures to ensure the security of personal data. In general, regulations to protect the security of personal information are often embodied in national laws. They are transferred at the beginning from general principles (such as transnational data protection principles) into a country's specific legal system. The core of international regulations is often principled, such as the Fair Information Privacy Principles proposed by the US Federal Trade Commission to protect online privacy. In financial, consumer and child protection field, United States promulgated several laws, such as The Children's Online Privacy Protection Act (COPPA), the K-12 Cybersecurity, etc. In December 1997, China promulgated the "Measures for the Administration of Internet Computer Information Network Security Protection" to strengthen the security protection of computer information networks. Since 2017, China has implemented the "Network Security Law" which stipulates the overall goals and basic objectives of the internet information security law in principle. Japan, United Kingdom, Australia, Brazil, South Africa and other countries have also introduced similar internet security protection regulations. Some non-governmental organizations (NGOs) such as the United Nations (UN), the Organization for Economic Cooperation and Development (OECD), the Asia-Pacific Economic Cooperation (APEC), and the International Organization for Standardization (ISO) have also issued laws, regulations, framework and principles, etc. related to personal data protection in different forms.

In various network protection frameworks and principles, Europe and the EU have strict requirements in the formulation of various laws and regulations. For example, for the European Convention on Human Rights and Article 8 of the Charter of Fundamental Rights of the European Union, the fundamental rights to the protection of personal information are clarified. In 2018, the European Union enacted the world's most stringent personal information protection law - the General Data Protection Regulation (GDPR), which regulates how companies collect, use and process personal data of EU citizens. These have played a very positive role in protecting the operation of education and teaching platforms in EU countries and partner countries.

The research project entitled "Research on the design and practice of blended teaching from the perspective of internationalization at home in the post-epidemic era" is supported by the Foundation of 2021 Planning Research Project of Shanghai Higher Education Association with No. Y2-24.

[1] 'Emergency' for global education, as fewer than half world's students cannot return to school [Online]. Available: https://news.un.org/zh/story/2020/08/1065822

[2] UNESCO Institute for Statistics, WHAT'S NEXT? LESSONS ON EDUCATION RECOVERY: FINDINGS FROM A SURVEY OF MINISTRIES OF EDUCATION AMID THE COVID-19 PANDE. United Nations Educational, Paris: Scientific and Cultural Organization, June 2021.

[3] Countries urged to reopen classrooms, assess pandemic-related learning loss [Online]. Available: https://news.un.org/en/story/2021/07/1095742

978-1-6654-8887-7/22/$31.00 ©2022 IEEE

With the development of E-learning platforms, the advantages and disadvantages of distance learning are gradually reflected. Callan (2010) and Garrison (2011) focused on many advantages of E-learning technology, including low cost and time saving, rich resources with different levels that match students' interests, learners can develop their own learning pace and effectively help them adjust by themselves in order to reduces stress and increases satisfaction. Similarly, other scholars have analyzed the disadvantage of online learning platforms. The research results of Holmes (2006) indicated that some teachers have little or none "personal" contact with students, the design of some E-learning platforms has technical problems, it makes students have a sense of isolation and feel no need to participate actively. Especially in developing countries, a lack of adequate E-learning strategies, technical experts, financial support, and student resistance to using e-learning systems also make online learning difficult.

Relatively speaking, with the support of advanced technology, Learning Management System (LMS) are developing earlier and faster in western countries. LMS is a software application for the administration, documentation, tracking, reporting, automation, and delivery of educational courses, training programs[4], materials or learning and development programs. Currently, some countries have built online teaching platforms with high technical content and features. These platforms are not only for presenting and sharing resources, but also provide interactive communication between teachers and students, or among students. Such as virtual chat rooms, electronic whiteboards, video conferences, etc. LMS has created a variety of ways to provide resources for students' learning. Not only that, the Internet also supports the transfer and use of multimedia elements. Various companies have developed different LMS for higher education through video and interactive hypermedia to facilitate online learning environments. With the help of LMS, teachers can be used manage courses, record students' learning process, and track students' learning. In specific teaching, LMS can provide online access to learning content not only for classroom teaching but also for blended learning, these are widely used in higher education. Nowadays, widely used LMS abroad includes Moodle, Blackboard, Canvas, Edmodo Google classroom, etc. In China, LMS such as Ketangpai, Rain Classroom and mosoteach are mainly used. Universities and schools in China are also prefer to developing their own LMS. With the strengthening of international cooperative education exchanges, the various online learning systems and platforms are integrated with each other, and widely used in teaching scenarios in Chinese universities in different ways.

III. DATA AND PRIVACY SECURITY RISKS IN LMS

Learning management systems in China and abroad have certain differences in interface setting, function division, and art design, but there is a huge common point - data and privacy security risks. Generally speaking, these risks exist in five aspects: personal devices and learning tools, registration and login modules, legacy account information, anti-virus tools and browsers, and the learning platform itself.

[4] RK Ellis, "Learning circuits'-Field guide to learning management systems," American Society for Training and Development (ASTD). Alexandria, VA, 2 009.

Figure 1. Data and privacy security risks in an LMS

A. Risks in Personal Devices and Learning Tools

Personal devices and learning tools are potential vectors of cyber risk. Before starting online learning, e-learners should prepare the equipment, network, download learning tools, read the privacy policy, etc. These not only help protect personal data, but also guarantee the quality of online learning. For students, parents, and teachers, if personal data stores on devices, data such as personally identifiable information may be at risk of loss or theft. if they are not properly managed, people will face network intrusions, man-in-the-middle attacks, and browser hijacking risks. Personal identification information and biometric information will face the threat of fake or malicious websites, computer viruses and malware when selecting and installing learning tools. Ignoring the importance of privacy policy when using various software and equipment, personal information may be exposed to risk of misuse by online learning tools.

B. Privacy Risks during Registration and Login

The risks of registering and logging in are also high. When users log in to the learning platform, they often need to register first, and privacy information may be leaked during this process. When creating account passwords, personally identification information and network identification information may be too simple and leading to password leakage. When using public equipment for online learning, there is a risk of personal data and privacy leakage. Using on public computer equipment especially in libraries, Internet cafes and airports are also not safe. There are also some phishing and plug-ins that allow users to automatically save their passwords when logging in, or call back login or logout data through caches and other methods, resulting in password leaking.

C. Data and Privacy Risks of Antivirus Software, Browsers and Firewalls

Antivirus software, browsers and firewalls are all essential parts of network usage. Antivirus software can avoid some security risks within a certain range. However, the differences in antivirus software development companies and source files used, as well as browser incompatibilities may have negative effects on students' study, such as personal information leakage, distraction, and addiction. The uncertainty of using anti-virus software will expose users to external attacks and lead to user

information leakage. Texts, photos, videos or website links published in social networks may contain personal privacy and data, resulting in the exposure of personal information. Some antivirus software will reject other similar antivirus tools as viruses by default, or directly delete the associated effective content, resulting in unnecessary loss of online learning materials.

D. Risk of Keeping Personal Data after Learning Online

After completing online learning for a period of time, users should pay attention to the data generated during the learning process. The data contains a large amount of personal identification information and network usage history. If the platform does not allow deletion or the account goes dormant, information will be left behind. The remaining information may be at risk of being abused by the learning platform. If the third-party of the online learning platform is attacked, information will be leaked, and even personal information will be illegally spread. Some users are also accustomed to using similar or identical passwords on different websites, software, APPs, and even bank accounts, which invisibly expands the daily risk of users.

E. Data and Privacy Risks on Online Learning Platform itself

After logging in to the learning platform, learners can sign up for courses, publish information on forums and blogs, browse and learn course content, but there is also the risk of personal data and privacy leakage and theft during online learning. The basic information, attendance information, preferences and learning records of course registration and management have the risk of data leakage caused by users, sites or third parties. Personal online records (such as user basic information, preferences and learning patterns, etc.) during personalized learning) will face the risk of extraction and malicious use. The risk of leakage due to external attacks on the platform, and the risk of the learning platform providing illegal information to third-party platforms. When studying online, people may often search on the Internet to create Internet browsing traces, this kind of searching sometimes may threaten your privacy. Therefore, people still need to pay attention to and protect the privacy during searching. Many applications on mobile phones or computers will ask for personal location information, and its misuse may cause the risk of personal information leakage. When a computer is attacked by malware, there is also a risk of file loss and corruption.

IV. NETWORK DATA PROTECTION FEATURES OF MOODLE-BASED "SHCNEO" E-LEARNING PLATFORM

As part of the " Transnational education – enhancement and excellence through profile building" funding program, the German Academic Exchange Service (DAAD) allocated a special fund to build the "SHCneo" online learning platform since June 2014. Through the development and operation of Moodle, SHCneo developer team is formed by the technical and management personnel from the University of Shanghai for Science and Technology (USST) in China and the Hamburg University of Applied Sciences (HAW Hamburg) in Germany. SHCneo is for supporting the cooperative educational institutions of the two universities - Shanghai-Hamburg College (SHC), which carries out online and offline blended learning education for multiple study courses.

Since EU promulgated the GDPR regulations in 2018, in order to allow students and teachers to have a safer online learning environment, SHCneo has clarified the following points when collecting personal data: first, only collect necessary personal data, effectively avoid the collection of personal data for purposes other more than legitimate purpose. Second, do not process personal data for purposes other than the legitimate purpose of collecting personal data. Third, delete personal data after achieving the legitimate purpose of collecting personal data to prevent information leakage caused by remaining information.

Moodle has also followed the GDPR principles after the regulations were enacted. First, a set of features was developed in Moodle 3.3 and Moodle 3.4 to help Moodle meet GDPR compliance requirements, and then the policy plugin and data privacy plugin were directly integrated in Moodle 3.5. Policy plugin allows to define various policy files (website policy, privacy policy, intellectual property policy, delayed allocation policy, etc.) and provides a new user login process, in order to be able to define multiple policy applicable objects, such as website, privacy, third parties, tracking users consent, and manage policy updates and version control. The data privacy feature provides users with a workflow for submitting subject access and deletion requests and for site administrators and data privacy officers to process those requests. It also includes a data registry, which defines the purpose and retention period of data stored in the Moodle site.

Based on the above principles, SHCneo implements the following measures.

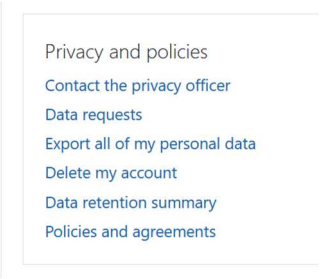

Figure 3. Privacy and policies section for users on SHCneo

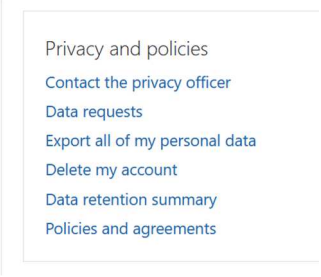

Figure 2. Privacy and policies section for administration on SHCneo

A. Upgrade the Moodle Version of SHCneo

After years of operation, the SHCneo platform project has updated a lot of secondary development codes. In order to maintain the stability of the system, the platform is still using the

"Moodle 2.9" version in 2018. In order to make the platform compliant with the GDPR regulations as soon as possible, the SHCneo platform underwent a major update in 2019, upgrading Moodle to version 3.3 and installing the corresponding GDPR plugin. Next, the SHCneo upgraded the Moodle to a more secure version 3.5 in 2020, and properly configure and implement the required processes and procedures.

B. *Check GDPR Compliance of the Third-party Plugins on SHCneo*

Many Moodle plug-in developers have added GDPR content to update after the promulgation of GDPR, SHCneo team only need to upgrade these plugins to meet the requirements of GDPR, such as CodeRunner, Etherpad Lite, H5P, etc. For custom-developed Moodle plugins, SHCneo team has to write custom code to comply with GDPR requirements, such as Javaunittest, WechatAuth. In addition, plugins that have not been used for a long time are deleted, such as Gismo, MOCLog2, etc.

C. *Set a Privacy Officer on SHCneo*

One of the functions of GDPR in the Moodle is to establish the role of privacy officer, responsible for processing user requests for data, including providing data or deleting data. SHCneo is jointly used by teachers and students from both China and Germany, and the data security of users is also the joint responsibility of both parties. Therefore, the responsibility of the SHCneo Privacy Officer is also jointly undertaken by the personnel of the two universities, they both respond to the management of data requests on SHCneo.

D. *Officially Issue Data Privacy Statement*

In 2022, after several rounds of discussions between Chinese and German universities, the content of data privacy statement on SHCneo was finally determined, and the function of signing the privacy statement was enabled on SHCneo. After logging in, the user can first see the display of the privacy statement page. The privacy statement of the SHCneo is mainly aimed at the common data risk points in the online learning platform. It clarifies how the data on SHCneo is stored and used in accordance with the GDPR, so that users can clearly understand the status of their personal privacy data in SHCneo.

V. Analysis of Risk Aversion in Network Data Protection of on SHCneo

Comparing the data and privacy security risks in LMS, we can see that the "SHCneo" platform has adopted data and privacy protection in the following aspects.

A. *Data Protection during Login and Registration*

Users can only have access to SHCneo content after the registration. By disabling guest login in site policy, enabling "Force user login for profile" to keep anonymous visitors and search engines away from user profiles. The legal basis for the processing of data during login and registration is Art. 6 paragraph 1 of GDPR.

During the login, registration and use of learning materials on SHCneo, the user account, IP address, and usage itself and the duration of the corresponding usage will be stored. This kind of storage is to protect users from misuse and other unauthorized use.

B. *Data and Privacy Protection during Navigating Learning Platforms*

The learning elements used and user data of exercises are very important data on the e-learning platform. SHCneo stores this data in order to display the learning progress and to restore the learning state when users access the site next time. The legal basis for this data processing is Art. 6 paragraph 1 of GDPR. Every time when someone accesses SHCneo and retrieves a file, data about this process is temporarily stored on the server and processed in logfiles. These data include: IP address, date and time of access, pages accessed, files transferred, operating system, browser used(type and version) and name of Internet access provider. The temporary storage of the IP address by the system is necessary to enable delivery of the platform content to the computer. To do this, IP address must be saved for the duration of the session. Storage in logfiles is done to ensure the functionality of the website, to optimize the content of the website and to ensure the security of the information technology systems. SHCneo will also not pass these data to third parties unless this is necessary to pursue legal claims. In addition, since the platform is jointly developed and used by Chinese and German universities, standard contractual clauses have also been signed with the University of Shanghai for Science and Technology to protect the security of user data.

C. *Data Protection in Learning Tools*

Cookies are text files that are stored in the internet browser or by the internet browser on users' computer system. SHCneo uses cookies to process data. The legal basis for this data processing is Article 6 Section 1 of GDPR. If users visit SHCneo, cookies can be stored on their operating system. These cookies contain a characteristic character string that enables the browser to be clearly identified when the website is visited again. Due to the local storage, users have full control over the use of cookies. Users can deactivate or restrict the transmission of cookies by changing the setting of internet browser. Also, Cookies that have already been saved can be deleted at any time. This can also be done automatically. If cookies are deactivated for website, it may no longer be possible to use all the functions of the website to their full extent.

The SHCneo platform contains two types of cookies - transient cookies and persistent cookies. These two cookies make SHCneo technically functional and user friendly. The first are transient cookies. Transient cookies are automatically deleted when users close the browser. On SHCneo, the so-called session cookie ("MoodleSession") represents such a transient cookie. It stores the session ID, with which various requests from the browser can be assigned to the joint session. This allows users' computer to be recognized when they return to SHCneo website. The session cookies are deleted when users log out or close the browser. This cookie is technically necessary for the platform. The second is persistent cookies. In contrast to transient cookies, persistent cookies are automatically deleted after a specified expiration time. On SHCneo, the "MOODLEID" cookie is such a persistent cookie. Its expiry period is one month. After the user agrees, it remembers the username in the browser, so that when the user returns to

SHCneo, the username field on the login page is already filled in.

Additionally, in order to be able to provide support efficiently and reliably, SHCneo uses Content Delivery Network (CDN) to provide certain services. The Privacy Statement also informs users that SHCneo uses CDN services, content such as Javascript programming libraries, fonts or style sheets is delivered faster and more reliably via regionally distributed servers connected to the Internet. Access data from users (log files such as IP addresses, access times, etc.) is also processed on the CDN servers.

D. Handling of Personal Data after Learning Online

On SHCneo, if users delete their user accounts, the data associated with that user account will also be deleted according to the deletion period of the backups. If the account is deleted, user has responsibility to make a backup of the required data before the end of use. Subject to the rights under the GDPR, SHCneo has the right to irretrievably delete all data stored during the period of use. The creation of the accounts, including usage activities (i.e. among other things, the learning progress) will be automatically deleted after 3 years of registration at the latest if they are inactive. Users will be informed 4 weeks in advance about the planned deletion and can actively object to it. For account information such as log files, these data will be deleted as soon as they are no longer required to achieve the purpose for which they were collected. When collecting the data for the provision of the website, this is the case when the respective session has ended. With regard to the storage of data in logfiles, this is the case after 14 days.

VI. CONCLUSION

With the deepening of the Internet age, the demand for online privacy protection in teaching platforms is becoming stronger and stronger. Through the network data evasion analysis of the "SHCneo" online learning platform, we can think and improve from the following aspects.

First, the necessity of module setting during platform development. In the development of an online teaching platform, the principle of practicality should be adopted, and the simplest and necessary modules should be set according to the needs of users.

Second, user prompts and data protection agreements. When the user registers and logs in, according to the requirements of the GDPR regulations, a data protection agreement that meets the specific requirements of the platform is set, and the user is required to register and log in after confirmation.

Third, increase the supervision and protection of background data. According to actual needs, set a thicker "protective clothing" for background data, even filter useless risk data and duplicate resources to ensure the integrity of user data.

Fourth, establish a linkage mechanism for online teaching platforms. Integrate online teaching platforms of different development systems, share educational and teaching resources, simplify the use process, and improve the efficiency of resource utilization.

Fifth, further improve the regulations on data privacy for special platforms. For special platforms like the "SHCneo" platform, eliminate loopholes in the system, maintain policy stability, and improve the level of data privacy protection.

REFERENCES

[1] V. I. Marín, J. P. Carpenter,G. Tur, “Pre-service teachers’ perceptions of social media data privacy policies,” British Journal of Educational Technology, Volume 52, Issue 2, Sept. 2020.

[2] L. Benade, From technicians to teachers: Ethical teaching in the context of globalized education reform,New York, NY/London, United Kingdom: Continuum,2012.

[3] C. Míguez-Álvarez, M. Cuevas-Alonso, M. I. Doval-Ruiz, Preservice Teachers’ Perceptions of Linguistic Abilities and Privacy Policies in the Use of Visual Materials During Their Own and Their Tutors’ Lessons, Frontiers in Education, 2022.

[4] P. Prinsloo, S. Slade, M. Khalil,“The answer is (not only) technological: Considering student data privacy in learning analytics,” British Journal of Educational Technology, Volume 53, Issue 4, April 2022.

[5] S. Noguerón-Liu,“Everybody Knows Your Business/Todo Mundo Se Da Cuenta: Immigrant Adults’ Construction of Privacy, Risk, and Vulnerability in Online Platforms,” Journal of Adolescent & Adult Literacy, Volume 60, Issue 5, September 2016.

[6] B. Paris, R. Reynolds, C. McGowan, “Sins of omission: Critical informatics perspectives on privacy in e-learning systems in higher education,” Journal of the Association for Information Science and Technology, Volume 73, Issue 5, September 2021.

[7] S. K. Almasoud, A. Almogren, M. M. Hassan, I. Alrassan, “An efficient approach of improving privacy and security in online social networks,” Concurrency and Computation: Practice and Experience, Volume 30, Issue 5, August 2017.

[8] S. Hutt, R. S. Baker, M. M. Ashenafi, J. M. Andres-Bray, “Christopher Brooks. Controlled outputs, full data: A privacy-protecting infrastructure for MOOC data,” British Journal of Educational Technology, Volume 53, Issue 4, May 2022.

[9] A. Aleksieva-Petrova, I. Chenchev, and M. Petrov. "LMS Data Collection, Processing and Compliance with EU GDPR." EDULEARN19 Proceedings, 2019.