UDC 004.678

K. Patsaliuk
S. Nykyporets

THE IMPORTANCE OF USER CONSENT AND PERSONAL DATA PROTECTION LAWS IN THE DIGITAL AGE

Vinnytsia National Technical University

Анотація

Розглянуто користувацький дозвіл на збирання та обробку особистої інформації, його типи та приклади. Проаналізовано регламенти та закони, що захищають право користувача на конфіденційність, які діють на територіях Європи та Сполучених Штатів Америки.

Ключові слова: кібербезпека, згода користувача, кукі, закони про захист даних, загальний регламент захисту даних.

Abstract

User permission to collect and process personal information, its types, and examples were considered. The regulations and laws protecting the user's right to privacy, which are in force in the territories of Europe and the United States of America, were analyzed.

Keywords: cybersecurity, user consent, cookies, data protection laws, General Data Protection Regulation (GDPR).

Introduction

Today people are living in a digital era, furthermore, they are often asked to exchange information about themselves, their preferences, and habits via different online platforms. With that being said, controlling how data is used and maintained, by whom, and why, becomes increasingly challenging.

To create a personalized experience for consumers, a website or organization must ask for user consent before accessing one's information. This gives companies insights into users' behavior on the website, allowing them to attract more customers and improve their advertising and marketing strategy.

Although user consent seems like a straightforward concept, it has taken on an immense level of importance with the evolution and growth of information technology. Modern technological, social, and legislative trends require the regulation of how information is collected and what control a data subject has over their information once it is transferred to ensure transparency and privacy between businesses and their customers.

This work aims to research user consent to process and use personal data, as well as current personal data protection laws.

Research results

Vast amounts of data are added to the internet and shared via connected devices every day. Digital technologies are used to create, process, store, and share information and data related to people, organizations, and governments.

Companies collect data to gain more detail into metrics such as sales, operational performance, customer service, and audience demographics. According to the National Commission on Informatics and Liberty (CNIL), personal data is "any information relating to an identified or identifiable individual" [1]. This definition includes many forms of information, such as names, postal and email addresses, telephone numbers, driver’s licenses, bank accounts, credit cards, passports, and Social Security numbers.

The data helps various companies understand the needs and desires of their customers when used properly. Furthermore, it serves as the basis for personalization and improving customer service. They also form the basis for automated and repeatable marketing processes that help companies evolve their operations [2].

However, before businesses can access users' personal data, they must now gain their consent. User consent is a fairly forthright concept. In simple terms, user consent is the permission granted by users to a website or organization to proceed with their data collection. Having said that, different countries have their legislations and interpretations of what constitutes valid ‘user consent’ and how it can be obtained.

Consent means to give an individual genuine choice and control over how their data is collected and used. That is to say, for consent to be considered valid and freely given, it must ensure that all of the given data is fully consented to and evidenced. This also means that any person has the right to refuse consent without detriment and be able to withdraw consent easily at any time.

A cookie consent banner is one of the ways to obtain the user's consent. The text, position, and design of the banner may differ, but its main purpose is to inform website users of the use of cookies on the website or to collect their consent for marketing purposes.

The first major reason why consent became essential is transparency. Before data protection legislations and laws were applied, businesses had unlimited access to data. Websites could target their visitors based on the information that the customer's device held, such as brand, operating system, language, time, etc., which ensured that ads were converted into purchases.

It was not uncommon for users who did not allow websites to have this access (consent to cookie tracking) would have a diminished user experience [3]. For instance, the need to log in each time a Facebook feed is refreshed or the empty shopping cart each time a person moves to another page would be discomforting. As a result, the prospect of a poor browsing experience was enough for users to accept cookie tracking. However, now users are guaranteed an equal or even better browsing experience on a site even if they accept only the necessary cookies for basic functions.

The amount of personal data around the world continues to rise, making it challenging for end users to know and protect the information they share. To govern the collection, use, disclosure, and care of personal data, privacy laws were created. These laws aim to give individuals control over their data, empowering them to know how it is being used, by whom, and why. Now organizations are obligated to take the necessary precaution to protect the data that they were trusted with. Data protection laws such as the CPRA, the GDPR, and LGPD have their own requirements for obtaining user consent online.

The General Data Protection Regulation (GDPR) was first introduced in May 2018 and has set a high bar for privacy protection for individuals within EU member states. GDPR is considered to be the world's strongest and toughest data protection and privacy law [4]. It enhances how people can access information about themselves and places limitations on what organizations can do with it. Europe’s privacy law requires companies to ask for some permission to share data and gives individuals rights to access, delete, or control the use of that data. GDPR is not the first privacy law, and it replaces the 1995 Data Protection Directive [5].

The United States lacks a single governing data protection piece of legislation like Europe's privacy law, the General Data Protection Regulation (GDPR). According to International Comparative Legal Guides, "a jumble of hundreds of laws enacted on both the federal and state levels serve to protect the personal data of U.S. residents" [6]. This is why personal data is generally collected and processed based on the data type under discussion. Another key thing to remember is that many types of data that GDPR covers do not have analogous protections under American law.

The United States' California Consumer Privacy Act (CCPA) is the most comparable to GDPR. It became effective in January 2020 and applied to California residents. The CCPA law allowed California consumers to request what information a company has saved on them and to demand to delete all of the sensitive data [7]. In addition, this law lets customers sue businesses if privacy principles are violated. However, the CCPA's successor, the California Privacy Rights Act (CPRA), introduced changes to the law that brought it even closer to GDPR.

The CPRA came into effect on January 1, 2023, and will become fully enforceable on July 1, 2023. It significantly amends the privacy legislation, expands, and renovates the CCPA, cleaning up indeterminacies. The California Privacy Rights Act creates a new category of personal information and changes the opt-out right to regulate cross-contextual behavioral advertising and its use of personal information, etc. Additionally, it makes a business responsible for how third parties use, share, or sell personal information that the business collected in the first place [8].

Data privacy laws were also enacted in Brazil. The General Data Protection Law (LGPD) (in Portuguese) became effective on August 1, 2021, and was also influenced by the European Union's General Data Protection Regulation (GDPR). This federal law is not the first or only data privacy law in South America. Its main purpose is to regulate the processing of personal information of individuals. The LGPD is made up of 65 articles, and it has expanded laws in some areas compared to the GDPR [9].

Conclusions

In today's digital era, consumer data is floating around the web while being shared with organizations, companies, and governments. Diverse businesses use this information to understand users' behavior, increase their sales, and promote ads to other potential customers, offering a personalized user experience and customer service in return. In conclusion, data privacy is a fundamental human right and data protection laws exist to defend that right. As personal information can be misused in a number of ways, data privacy laws aim to give the end user control over how their data is used, by whom, and why. Companies are now obligated to be more transparent about the collection and processing of consumer data and protect sensitive information against breaches.

Countries have set privacy legislation to govern data confidentiality and protection. All things considered, Europe's General Data Protection Regulation (GDPR) has become the world's strongest set of privacy protection rules. Many other data privacy regulations and legislations are now aligned with a European approach, such as California's Consumer Privacy Act (CCPA), its heir California Privacy Rights Act (CPRA), and Brazil's General Law for the Protection of Personal Data (LGPD).

To summarize, the data privacy landscape has changed considerably in recent years around the world and continues to expand consumer rights over the control of confidential data. As technologies evolve, new data privacy laws are being considered and enacted. Above all, it is essential to ensure that organizations all around the world comply with the existing privacy laws.

REFERENCES

1. Personal Data: definition | CNIL [Electronic resource] // CNIL |. – Mode of access: https://www.cnil.fr/en/personal-data-definition (date of access: 20.04.2023). – Title from screen.
2. Why is your personal data important and valued? [Electronic resource] // Bocasay. – Mode of access: https://www.bocasay.com/what-personal-data-worth-how-is-used/ (date of access: 23.04.2023). – Title from screen.
3. What does user consent mean and why does it matter? – security [Electronic resource] // Security. Mode of access: https://securiti.ai/blog/user-consent/ (date of access: 28.04.2023). – Title from screen.
4. GDPR archives - gdpr.eu [Electronic resource] // GDPR.eu. – Mode of access: https://gdpr.eu/tag/gdpr/ (date of access: 30.04.2023). – Title from screen.
5. The History of the General Data Protection Regulation [Electronic resource] // European Data Protection Supervisor. – Mode of access: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en (date of access: 30.04.2023). – Title from screen.
6. Data Protection Laws and Regulations Report 2022-2023 USA [Electronic resource] // International Comparative Legal Guides International Business Reports. – Mode of access: https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa (date of access: 04.05.2023). – Title from screen.
7. California Consumer Privacy Act (CCPA) [Electronic resource] // State of California - Department of Justice - Office of the Attorney General. – Mode of access: https://oag.ca.gov/privacy/ccpa(date of access: 04.05.2023). – Title from screen.
8. California Privacy Rights Act – CPRA and CCPA – Cookiebot™ [Electronic resource] // Cookiebot. – Mode of access: https://www.cookiebot.com/en/cpra/(date of access: 01.05.2023). – Title from screen.
9. LGPD Brazil – General Personal Data Protection Act [Electronic resource] // LGPD Brazil – General Personal Data Protection Act. – Mode of access: https://lgpd-brazil.info(date of access: 04.05.2023). – Title from screen.

Пацалюк Каріна Вадимівна — студентка групи УБ-21б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: karina_vin@icloud.com

Науковий керівник: ***Никипорець Світлана Степанівна*** — викладач англійської та німецької мов, кафедра іноземних мов, Вінницький національний технічний університет, м. Вінниця

Patsaliuk Karina V. — Faculty of Management and information security, Vinnytsia National Technical University, Vinnytsia, email: karina_vin@icloud.com

Supervisor: ***Nykyporets Svitlana S.*** — Teacher of English, Department of Foreign Languages, Vinnytsia National Technical University, Vinnytsia