UDC 347.41:342.9:334.716:004.056
DOI https://doi.org/10.32782/2524-0374/2023-6/150

DATA PRIVACY AND SECURITY: LEGAL OBLIGATIONS FOR BUSINESSES IN THE DIGITAL AGE

КОНФІДЕНЦІЙНІСТЬ ТА БЕЗПЕКА ДАНИХ: ЮРИДИЧНІ ЗОБОВ'ЯЗАННЯ ДЛЯ БІЗНЕСУ В ЦИФРОВУ ЕПОХУ

Tuz A-M.V., 4-th year Student
Institute of Law of Taras Shevchenko National University of Kyiv

This article provides an overview of the legal obligations of businesses to protect data privacy and security in the digital age. It begins with an overview of the digital era and its impact on data privacy and security. It then highlights the importance of businesses complying with their legal obligations in relation to the processing of customer data.The legal framework for data privacy and security is then examined. An overview of the main data protection laws such as the GDPR and CCPA is provided. The key provisions and requirements of these laws are explained. Jurisdictional aspects and the global impact of the legislation are also highlighted.

The specific legal obligations of businesses to protect data privacy and security are examined. It discusses consent and notification requirements for data collection and processing, emphasising the importance of voluntary and informed consent. It also explores the principles of transparency and accountability, the rights of data subjects and the obligation to notify individuals promptly in the event of a data security breach. The article explores the problems of compliance and the risks of failure to fulfil legal obligations. The author points out the possible legal consequences for failure to comply with data protection rules. It also discusses new challenges and future trends in the field of data privacy and security. The article concludes with practical recommendations: the importance of establishing a comprehensive data privacy and security programme, training employees on data protection and cybersecurity, and engaging reliable service providers with effective data protection measures. In summary, the article emphasises the need to comply with legal obligations in the field of data protection for businesses in the digital age. The application of recommendations and best practices, as well as a proactive approach to data protection compliance, will help businesses adapt to the changing landscape of data privacy and security, mitigate risks and ensure compliance with legal requirements.

Key words: data privacy, cybersecurity, business, data protection, confidentiality.

Стаття присвячена огляду правових зобов'язань бізнесу щодо захисту приватності та безпеки даних у цифрову епоху. Вона розпочинається оглядом цифрової ери та її впливу на приватність та безпеку даних. Акцентується увага на важливості дотримання правових обов'язків бізнесом щодо обробки даних клієнтів. Далі розглядається законодавча рамка для захисту приватності та безпеки даних. Надається огляд основних законів про захист даних, таких як GDPR та CCPA. Пояснюються ключові положення та вимоги цих законів. Також звертається увага на юрисдикційні аспекти та глобальний вплив законодавства.

Розглядаються конкретні правові зобов'язання бізнесу щодо захисту приватності та безпеки даних. Обговорюються вимоги щодо отримання згоди та повідомлення про збір та обробку даних, підкреслюючи важливість добровільної та обізнаної згоди. Також досліджуються принципи прозорості та відповідальності, права суб'єктів даних та зобов'язання швидко повідомляти осіб у разі порушення безпеки даних. Стаття досліджує проблеми виконання та ризики від невиконання правових зобов'язань. Вказується на можливі правові наслідки за невиконання правил захисту даних. Також розглядаються нові виклики та майбутні тенденції в області приватності та безпеки даних. Завершується стаття практичними рекомендаціями: зазначається важливість створення комплексної програми захисту приватності та безпеки даних, навчання працівників щодо захисту даних та кібербезпеки, а також залучення надійних постачальників послуг з ефективними заходами захисту даних. Узагальнюючи, стаття підкреслює необхідність дотримання правових зобов'язань у сфері захисту даних для бізнесу в цифрову епоху. Застосування рекомендацій та найкращих практик, а також проактивний підхід до виконання правил захисту даних, допоможуть бізнесу пристосуватися до змінюючогося ландшафту приватності та безпеки даних, зменшити ризики та забезпечити відповідність правовим вимогам.

Ключові слова: приватність даних, кібербезпека, бізнес, захист даних, конфіденційність.

Introduction. The digital age has brought about an unprecedented transformation in the way businesses operate and interact with customers. With the proliferation of digital technologies, organizations have gained access to vast amounts of data that can drive innovation, enhance decision-making, and improve customer experiences. However, this digital revolution has also raised significant concerns about data privacy and security.

In today's interconnected world, personal and sensitive information is constantly being exchanged and stored digitally. From online transactions and social media activities to healthcare records and financial data, individuals entrust businesses with their personal information, expecting it to be handled with the utmost care and protection. However, the rapid advancement of technology and the increasingly sophisticated nature of cyber threats have exposed this data to new risks.

The impact of data breaches and privacy violations has reverberated worldwide, eroding trust in businesses and undermining individuals' confidence in the digital ecosystem. As a result, governments and regulatory bodies have responded by introducing stringent data protection laws and regulations, placing legal obligations on businesses to safeguard customer data and uphold the fundamental right to privacy.

The importance of legal obligations for businesses in handling customer data cannot be overstated. Compliance with data protection laws not only ensures that organizations meet their legal responsibilities but also contributes to building and maintaining trust with customers. By prioritizing data privacy and security, businesses can demonstrate their commitment to protecting individuals' rights and mitigating the risks associated with data breaches and cyber threats.

In this scientific article, we delve into the legal obligations that businesses face in safeguarding customer data in the digital age. By examining relevant legislation and regulations, we aim to provide a comprehensive understanding of the responsibilities businesses have and the measures they should adopt to uphold data privacy and security. By fulfilling these obligations, businesses can not only comply with the law but also foster a culture of trust, transparency, and accountability that is essential in the digital landscape.

Legislative Framework for Data Privacy and Security. The GDPR, enacted by the European Union (EU) in 2018, has established a comprehensive framework for data protection and privacy. It applies to businesses that process personal data of individuals within the EU, regardless of the business's location. The key provisions and requirements of the GDPR include:

a. Extraterritorial Scope: The GDPR has an extraterritorial reach, meaning it applies to businesses outside the EU if they offer goods or services to EU residents or monitor their behavior.

b. Lawful Basis for Processing: Businesses must have a lawful basis for processing personal data, such as consent, contractual necessity, legal obligation, vital interests, public task, or legitimate interests.

c. Data Subject Rights: The GDPR grants individuals several rights, including the right to access, rectify, erase, and restrict processing of their personal data. It also provides for data portability and the right to object to automated decision-making.

d. Consent: Consent must be freely given, specific, informed, and unambiguous. Businesses must obtain clear consent before processing personal data, and individuals have the right to withdraw consent at any time.

e. Data Breach Notification: Organizations must report data breaches to the relevant supervisory authority within 72 hours of becoming aware of the breach, unless it is unlikely to result in risks to individuals' rights and freedoms [1, p. 17].

Another important document is California Consumer Privacy Act (CCPA). The CCPA, enacted in 2018, is a significant data privacy law in the United States. It applies to businesses that collect and process personal information of California residents and meet certain revenue or data processing thresholds. The key provisions and requirements of the CCPA include:

a. Scope and Applicability: The CCPA applies to businesses that meet specific criteria, including annual gross revenues exceeding a certain threshold or handling the personal information of a certain number of California residents

b. Consumer Rights: The CCPA grants California residents various rights, such as the right to know what personal information is collected, the right to request deletion of personal information, and the right to opt-out of the sale of personal information.

c. Notice and Transparency: Businesses must provide clear and easily accessible notices to consumers regarding the collection, use, and sharing of their personal information. The notices must disclose the purposes for data collection and the categories of third parties with whom the data is shared.

d. Data Protection Measures: The CCPA requires businesses to implement reasonable security measures to safeguard personal information and protect it from unauthorized access, disclosure, or destruction.

Data privacy laws have implications beyond their local jurisdictions. The extraterritorial scope of laws like the GDPR means that businesses worldwide must comply with their provisions when processing data of individuals in covered regions. Consequently, businesses operating in multiple jurisdictions face the challenge of navigating varying legal requirements and ensuring compliance across different regulatory landscapes [2, p. 8].

The impact of these data protection laws extends beyond their respective regions. Many countries and regions have taken inspiration from the GDPR and implemented or proposed their own data protection laws with similar principles and requirements. This global trend highlights the increasing recognition of the importance of data privacy and security and reflects the need for businesses to adopt consistent practices to protect personal data regardless of their location. Understanding the legislative frameworks, such as the GDPR and the CCPA, is essential for businesses to ensure compliance with data protection laws and meet their legal obligations. By adhering to these laws, businesses can enhance customer trust, minimize legal risks, and demonstrate a commitment to responsible data handling in the digital age.

Legal Obligations for Businesses. Ensuring data privacy and security is not only an ethical responsibility but also a legal requirement for businesses operating in the digital age. To comply with the law and protect individuals' rights, businesses must fulfill specific legal obligations related to data privacy and security. Below we will explore some key obligations that businesses need to address.

One fundamental legal obligation is obtaining appropriate consent from individuals before collecting and processing their personal data. It is crucial for businesses to ensure that consent is obtained in a clear, specific, and informed manner, providing individuals with sufficient details about the purposes and scope of data processing. Consent should be freely given, and individuals should have the option to withdraw their consent at any time.

Additionally, businesses must provide individuals with clear and transparent notices regarding their data collection and processing practices. These privacy notices should outline the types of data collected, the purposes for processing, any third parties involved, and the rights individuals have regarding their data. Adequate notice ensures transparency and enables individuals to make informed decisions about sharing their personal information.

Businesses have an obligation to be transparent and accountable for their data handling practices. This includes establishing and maintaining comprehensive data protection policies and procedures that align with relevant legal requirements. By implementing privacy by design and default principles, businesses should proactively integrate data protection measures into their operations and systems.

To ensure accountability, businesses should appoint a data protection officer (DPO) or designate a responsible person within the organization to oversee data privacy and security matters. This individual or team should monitor compliance with data protection laws, provide guidance to employees, conduct data protection impact assessments, and serve as a point of contact for data subjects and regulatory authorities [3, p. 198].

Data protection laws grant individuals certain rights regarding their personal data. Businesses have an obligation to respect and fulfill these rights. Some of the key rights include the right to access their personal data, the right to rectify inaccurate information, the right to erasure (or "right to be forgotten"), and the right to data portability. Businesses must have processes in place to enable individuals to exercise these rights and respond promptly and appropriately to such requests.

Moreover, businesses must ensure that they have appropriate mechanisms to verify the identity of individuals making data subject requests. This helps prevent unauthorized access to personal data and ensures that the rights of the rightful data subjects are respected.

Data breaches are a significant concern for businesses and individuals alike. In the event of a data breach, businesses have an obligation to promptly notify the affected individuals and, in some cases, the relevant regulatory authorities. The notification should include details about the nature of the breach, the types of data involved, and recommended actions for individuals to mitigate potential harm. Establishing an incident response plan and regularly testing it can help businesses respond swiftly and effectively to data breaches.

Businesses should also take steps to prevent data breaches by implementing appropriate technical and organizational measures. This includes regularly assessing and updating their security protocols, conducting risk assessments, and providing ongoing training and awareness programs to employees regarding data privacy and security best practices. By fulfilling these legal obligations, businesses can demonstrate their commitment to protecting data privacy and security, building trust with customers, and mitigating the risks associated with data breaches and privacy violations [4, p. 10].

Compliance Challenges and Risks. Complying with data privacy and security regulations poses various challenges for businesses in the digital age. These challenges come with inherent risks that businesses need to address.

One major challenge is the complexity of the regulatory landscape. Data privacy and security regulations differ across jurisdictions, making it difficult for businesses operating globally to navigate and ensure compliance with multiple sets

of laws. Understanding the nuances of each regulation, such as the GDPR, CCPA, and others, requires significant resources and expertise.

Another challenge is the evolving nature of technology. Technology is constantly advancing, and businesses must adapt their data privacy and security practices accordingly. However, keeping up with technological advancements, such as cloud computing, Internet of Things (IoT), and artificial intelligence (AI), presents challenges. Businesses must ensure that their data protection measures are up to date and can address the unique risks associated with emerging technologies.

Businesses often rely on third-party vendors and service providers to handle and process data. However, entrusting data to third parties introduces additional risks. Businesses must carefully assess the data protection practices of their vendors and ensure that appropriate contractual agreements are in place to protect the data and mitigate potential risks.

Data breaches and cybersecurity threats pose significant risks to businesses and individuals. The cost of data breaches can be substantial, including financial losses, reputational damage, and legal consequences. Businesses must implement robust cybersecurity measures, conduct regular risk assessments, and develop incident response plans to mitigate the risks associated with data breaches and cyberattacks.

International data transfers also present challenges. Global businesses often need to transfer data across borders. However, different jurisdictions have different requirements for cross-border data transfers. Businesses must navigate these restrictions and implement appropriate safeguards, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), to ensure lawful and secure international data transfers.

Non-compliance with data privacy and security regulations can lead to severe legal consequences for businesses. Regulatory authorities have the power to impose fines, penalties, and sanctions for violations. For instance, under the GDPR, non-compliance can result in fines of up to 4% of the annual global turnover or €20 million, whichever is higher. Moreover, non-compliance can result in reputational damage, loss of customer trust, and potential lawsuits from affected individuals. The negative impact on business operations and financial stability can be significant. Therefore, businesses must prioritize compliance efforts to avoid legal consequences and maintain their reputation in the market [5, p. 42].

Emerging Issues and Future Trends in Data Privacy and Security. Data privacy and security continue to be evolving areas, and businesses must stay informed about emerging issues and future trends. This proactive approach is crucial to effectively manage risks and protect data. Several key areas are shaping the future of data privacy and security:

a. Increased Regulatory Focus: Regulatory authorities worldwide are placing a stronger emphasis on data privacy and security due to growing public concern. Businesses can expect stricter enforcement, new regulations, and enhanced scrutiny in the coming years. Staying up to date with regulatory developments and adjusting compliance strategies accordingly will be crucial. This includes understanding the impact of regional regulations, such as the GDPR, CCPA, and other emerging frameworks, on data processing practices and ensuring compliance across different jurisdictions.

b. Artificial Intelligence and Machine Learning: The use of AI and machine learning technologies presents unique challenges for data privacy and security. Businesses must address issues related to algorithmic bias, explainability, and data protection in AI-driven systems. As AI becomes more integrated into various aspects of business operations, organizations must implement privacy-by-design principles and adopt robust privacy-preserving techniques. This involves ensuring transparency and fairness in AI algorithms, implementing data anonymization and encryption methods, and establishing data governance frameworks that encompass AI models and applications.

c. Data Ethics and Governance: Businesses are increasingly being held accountable for ethical data practices. Establishing robust data governance frameworks and promoting responsible data handling practices will become more important. This includes defining clear policies and procedures for data collection, use, and retention, as well as ensuring compliance with ethical principles, such as data minimization, purpose limitation, and user consent. Organizations should prioritize transparency and accountability in their data practices, fostering a culture of responsible data stewardship throughout the organization.

d. Privacy-Enhancing Technologies: Privacy-enhancing technologies are gaining attention as tools to strengthen data privacy and security. These technologies aim to provide privacy protections while enabling data analysis and sharing. Differential privacy, homomorphic encryption, and secure multiparty computation are examples of privacy-enhancing technologies that allow for data analysis while preserving privacy. Businesses should explore and adopt these technologies where appropriate to enhance data protection and maintain compliance with evolving regulations. Embracing privacy-enhancing technologies can offer a competitive advantage by demonstrating a commitment to privacy and security.

e. Data Localization and Sovereignty: Some jurisdictions are considering or implementing data localization laws that require businesses to store and process data within their borders. This trend raises concerns about cross-border data transfers and compliance with various legal frameworks. Businesses should closely monitor developments in data localization regulations and assess the impact on their operations. Implementing data governance strategies that address data residency requirements and incorporating privacy-preserving techniques can help navigate these challenges.

By staying proactive, adapting to emerging issues, and keeping abreast of future trends, businesses can navigate the evolving landscape of data privacy and security, mitigate risks, and ensure compliance with legal obligations. Taking a comprehensive approach to data privacy and security not only protects businesses from potential legal consequences but also fosters trust with customers and stakeholders in the digital age. Organizations that prioritize privacy and security will be better positioned to succeed in a data-driven world [6, p. 18].

Best Practices and Recommendations. To effectively address data privacy and security in the digital age, businesses should adopt best practices and implement recommended measures. By establishing a comprehensive data privacy and security program, training employees on data protection and cybersecurity awareness, and engaging third-party vendors with robust data protection measures, businesses can enhance their data privacy and security practices [7, p. 17].

a. Establishing a Comprehensive Data Privacy and Security Program: Businesses should develop and implement a comprehensive data privacy and security program that encompasses policies, procedures, and technical safeguards. This program should be tailored to the specific needs and risks of the organization and aligned with applicable data protection regulations. It should include clear guidelines on data collection, processing, retention, and disposal, as well as mechanisms to ensure compliance with privacy laws. Regular risk assessments, privacy impact assessments, and audits should be conducted to identify vulnerabilities and address them promptly. The program should also incorporate incident response plans and procedures to effectively handle and mitigate the impact of data breaches or security incidents.

b. Training Employees on Data Protection and Cybersecurity Awareness: Employees play a crucial role in maintaining data privacy and security. Businesses should provide comprehensive training programs to educate employees about data protection principles, cybersecurity best practices, and their role in safeguarding sensitive information. Training should cover topics such as recognizing and reporting security threats,

understanding phishing attempts, practicing secure data handling, and adhering to privacy policies and procedures. Ongoing training and awareness initiatives will help cultivate a privacy and security-conscious culture within the organization.

c. Engaging Third-Party Vendors with Robust Data Protection Measures: Many businesses rely on third-party vendors and service providers for various functions that involve handling personal data. When engaging such vendors, it is essential to conduct due diligence to assess their data protection practices. This includes evaluating their security measures, privacy policies, and compliance with relevant regulations. Businesses should establish strong contractual agreements that clearly define the obligations of the vendor regarding data protection and security. Regular monitoring and audits should be conducted to ensure ongoing compliance by the vendor. It is crucial to select vendors that prioritize data privacy and security and align with the organization's commitment to protecting customer information.

d. Data Minimization and Retention Policies: Implementing data minimization practices and establishing clear data retention policies are essential steps in protecting personal data. Businesses should only collect and retain the data necessary to fulfill specific purposes and delete or anonymize data that is no longer required. By adopting a data minimization approach, organizations can reduce the risk associated with storing unnecessary data and limit their exposure in case of a data breach or security incident.

e. Regular Security Assessments and Updates: Businesses should conduct regular security assessments to identify vulnerabilities and address them promptly. This includes evaluating the effectiveness of technical safeguards, such as firewalls, encryption, and access controls, and implementing necessary updates and patches to address known security vulnerabilities. Regular security testing, such as penetration testing and vulnerability scanning, can help identify potential weaknesses and proactively address them.

f. Privacy by Design and Default: Incorporating privacy by design and default principles into product and service development processes is crucial. Privacy considerations should be integrated from the initial design phase, ensuring that privacy controls and safeguards are built into the architecture and functionality of the systems. By default, the highest privacy settings should be applied to protect user data, allowing individuals to have control over their personal information.

By implementing these best practices and recommendations, businesses can strengthen their data privacy and security posture, reduce the risk of data breaches, and build trust with customers and stakeholders. Prioritizing data protection is not only a legal obligation but also a strategic advantage in the digital age where data privacy and security are paramount concerns [8, p. 94].

In conclusion, businesses must recognize that data privacy and security are paramount in the digital age. By adhering to legal obligations, establishing comprehensive data privacy and security programs, training employees, engaging trustworthy third-party vendors, and staying proactive in compliance efforts, businesses can navigate the complex landscape of data protection. Proactive compliance not only mitigates legal risks but also fosters customer trust and ensures a competitive advantage in today's data-driven world. As data privacy and security continue to evolve, businesses must remain vigilant, adaptable, and committed to protecting the privacy and security of customer data.

REFERENCES

1. Andrew Charlesworth, 'Clash of the Data Titans? US and EU Data Privacy Regulation', (2000), 6, *European Public Law*. Issue 2, pp. 253–274. https://kluwerlawonlinecom.ezp.sub.su.se/JournalArticle/European+Public+Law/6.2/265901

2. Krystyna Kowalik-Banczyk, 'Book Review: Data Privacy Law. An International Perspective, by Lee A. Bygrave. (Oxford: Oxford University Press, 2014)', (2015), 21, *European Public Law.* Issue 1, pp. 209–212, https://kluwerlawonline-com.ezp.sub.su.se/JournalArticle/European+Public+Law/21.1/EURO2015010

3. European Union General Data Protection Regulation (GDPR) – Official website: https://gdpr.eu/

4. California Consumer Privacy Act (CCPA) – Official website : https://oag.ca.gov/privacy/ccpa

5. Federico Ferretti, 'Data protection and the legitimate interest of data controllers: Much ado about nothing or the winter of rights?', (2014), 51, Common Market Law Review, Issue 3, pp. 843-868, https://kluwerlawonline-com.ezp.sub.su.se/JournalArticle/Common+Market+Law+Review/51.3/COLA2014063

6. Ceyhun Necati Pehlivan, 'Editorial: Privacy in Challenging Times', (2021), 2, *Global Privacy Law Review*. Issue 1, pp. 2–7, https://kluwerlawonline-com.ezp.sub.su.se/JournalArticle/Global+Privacy+Law+Review/2.1/GPLR2021001

7. Xin Wang, 'Online Personal Data Protection and Data Flows Under the RCEP: A Nostalgic New Start?', (2022), 56. *Journal of World Trade*, Issue 4, pp. 657–692, https://kluwerlawonline-com.ezp.sub.su.se/JournalArticle/Journal+of+World+Trade/56.4/TRAD2022027

8. Kerianne Wilson, 'Gone With the Wind?: The Inherent Conflict between API/PNR and Privacy Rights in an Increasingly Security-Conscious World', (2016), 41. *Air and Space Law*. Issue 3, pp. 229–264, https://kluwerlawonline-com.ezp.sub.su.se/JournalArticle/Air+and+Space+Law/41.3/AILA2016019