Data Protection from A Global Perspective: Challenges and Strategies for Multinational Corporation Data Security Compliance

Yiyang Jiang

Shanghai University of Political Science and Law, Shanghai, China
guqq@shanghaitech.edu.cn

Abstract. In recent years, data technology has been developing rapidly, and the free flow of data across borders has also brought about many risks and hidden dangers, such as data security issues, personal information protection, and corporate information compliance issues. This paper explores how multinational corporations manage these challenges through effective data protection strategies from a global perspective. It focuses on the current challenges of data compliance across various legal frameworks and the development of effective governance strategies. Two case studies are examined to highlight the practical difficulties and complexities encountered in international data security efforts. These examples illustrate the underlying causes of compliance failures and help set the groundwork for proposing more robust data compliance strategies. The findings from this research are intended to enrich the discourse on enhancing data security measures and compliance strategies, providing multinational corporations with actionable insights to navigate complex international data protection regulations and strengthen their data security protocols.

Keywords: Data Security, Multinational Corporations, Compliance.

1 Introduction

As more company activities become automated and an increasing number of computers are utilized to hold sensitive data, the necessity for secure computer systems grows. This necessity becomes particularly more apparent as applications and networks become established and accessible over an unprotected network, such as the Internet. The Internet has grown to be indispensable for businesses, financial institutions, governments, and countless daily consumers. Computer networks facilitate a diverse array of activities, the lack of which would essentially incapacitate these companies. Consequently, in the field of information technology, data security has been and will continue to be a serious concern [1].

The burgeoning volume of data necessitated for business operations presents companies with novel challenges, compounded by the rapid evolution of technology, the establishment of new compliance mandates, and the escalating demand for real-time information accessibility. Over 4.1 billion records were exposed as a result of more

B. Siuta-Tokarska et al. (eds.), *Proceedings of the 2024 2nd International Conference on Management Innovation and Economy Development (MIED 2024)*, Advances in Economics, Business and Management Research 300,
https://doi.org/10.2991/978-94-6463-542-3_39

than 3,600 data breaches in the first half of 2019. Given that data security breaches have affected firms such as Facebook, Microsoft, Amazon, and Adobe, and that the mean expense associated with a data breach amounts to $3.92 million, it is obvious that all businesses should place a high premium on data security [2].

Given the virtual nature of data that is easy to replicate, multinationals, as the primary actors in global economic activity, have a crucial responsibility in safeguarding data security. Data security is difficult to guarantee, especially for international enterprises. Craig Williams, the Director of Outreach at Talos, a cybersecurity company owned by Cisco, asserted in a recent video that the company blocks 20 billion threats daily, or close to three units per capita worldwide. Additionally, Forbes projects that by 2021, the yearly global cost of cybercrime will reach $6 trillion [3]. It's apparent that businesses need security measures in place to guarantee the confidentiality, availability, and integrity of their data. The myriad challenges encompass illegal data collection, usage, and storage leading to hefty fines or even operational cessation for enterprises; external threats like hacking and data breaches; and the onerous costs of compliance alongside grave risks of internal data leaks. Against this backdrop, navigating these risks and challenges to ensure stable and prosperous enterprise development in a competitive market encapsulates the essence of enterprise data compliance. Effective data compliance not only cultivates substantial business value for enterprises but also safeguards them from legal perils and galvanizes them to proactively fulfill their social responsibility.

This paper will unfold in structured parts, initially framing the critical importance of data security in the digital age and highlighting the pivotal role it will play across governments, corporations, and individual entities. It will progress to dissect the complexities of the global legal landscape for data protection, spotlighting the challenges multinational corporations will face in navigating diverse legal frameworks. A closer examination of compliance and operational hurdles will follow, including the financial impacts and strategic dilemmas corporations will encounter. The paper will then transition to discussing technological and managerial solutions aimed at fortifying data security measures and ensuring adherence to international standards. Concluding, it will offer targeted recommendations for enhancing data security and compliance strategies, equipping multinational corporations with insights to thrive amidst the challenges of a globally connected digital ecosystem.

2 Analysis of the Current Challenges

2.1 Diversity of Global Legal Standards

Data security is defined similarly across the legal literature, case law, and industry: it generally means institutional rules and technical methods that an institution utilizes to ensure that data is only accessed by authorized personnel. [4]. As digital globalization progresses, the pressing need for a new international governance consensus and framework on information and data security becomes evident to ensure stable international relations. The task of aligning global perspectives on cross-border data flows is chal-

lenging due to complexities involving data sovereignty, privacy, security, and legal jurisdictions. Currently, there's a lack of universal agreement on information security, with countries defining security based on individual interests, leading to significant policy and regulation disparities. This absence of consensus complicates the management of multinational enterprises, as they navigate the intricacies of international cooperation and legal compliance across diverse regulatory landscapes, highlighting the inherent conflicts in harmonizing different legal systems.

Existing Legislation in Different Countries.

From one region of the world to another, the landscape of data protection legislation is drastically different, marked by initiatives such as the European Union's General Data Protection Regulation (GDPR), effective from May 25, 2018, and California's Consumer Privacy Act (CCPA), implemented in 2020, followed by its successor, the California Consumer Privacy Rights Act (CPRA). Similarly, Virginia, Colorado, Utah, and Connecticut have established uniform personal data protection laws, reflecting a growing trend towards enhancing data privacy. Internationally, Japan updated its Personal Information Protection Law in 2020, effective April 2022, and Canada introduced the Digital Charter Implementation Act in November 2020. China’s Personal Information Protection Law (PIPL), coming into force on November 1, 2021, provides a comprehensive framework for data privacy, transitioning from a fragmented approach to a more unified legislation [5].

These developments underscore a leadership role played by developed regions, particularly Europe and the United States, in shaping global data protection standards. The EU's GDPR focuses extensively on personal data protection, setting a benchmark for others. The United States, through bilateral agreements and regional cooperation, promotes a model of cross-border data regulation. However, this diversity in laws and approaches poses significant compliance challenges for multinational corporations, grappling with varying legal models, regulatory practices, and data protection standards across jurisdictions.

Challenges in Legal Application and Enforcement.

The application and enforcement of legal standards for data protection present multifaceted challenges, especially in the context of differing objectives among states, societies, and enterprises. Although supported by appropriate laws and regulations, in the process of cybersecurity governance, the state attaches importance to security and stability, the society focuses on value realization and privacy protection, and enterprises pay more attention to economic benefits. This divergence complicates cross-border data governance, making the task of managing data security under multiple management frameworks without compromising interests a significant challenge for multinational corporations. Additionally, the necessity for governments to bolster regulatory efforts for data security, while navigating the complexities of internationalization, adds another layer of difficulty.

The endeavor to align multinational corporations' operations with global data compliance standards, such as the GDPR, illustrates these challenges. Despite the GDPR's

aim to standardize data protection across the EU and offer guidance for compliance, its practical application often reveals gaps, particularly in harmonizing with local laws outside the EU. The GDPR's initial promise to promote a consistent method of data management and the deployment of automation tools within enterprises often falls short in practice. Many enterprises find that, over time, the systems established for global compliance are more formalistic than functional, struggling to integrate with local legal requirements and failing to be fully adopted into the businesses' operational and management processes.

Challenges of International Cooperation and Coordination.

In the field of international cooperation, multilateral cooperation is difficult to achieve and regional cooperation has become a trend. The US and the EU are the two major economies of the world, with close ties to each other in many political, economic, social, and cultural fields. Nowadays, the United States and the European Union have long worked closely together on cross-border data flows, but both seek to take the lead in setting cross-border data flow standards, resulting in numerous rounds of intense games between the two sides. At the global level, this creates a collision and conflict of data governance claims, which in turn creates a series of challenges for the advancement of global data governance.

2.2 Compliance Challenges Faced by Multinational Companies

Risks of Transferring Data Across Borders.

Cross-border data flows in the digital age underpin globalized activities and are reshaping competitive labor market relations and value chains across countries. The dramatic growth of cross-border data flows far exceeds the growth of goods and services [6]. According to McKinsey, a 10% increase in data flow will drive a 0.2% increase in GDP [7]. It is anticipated that the financial worth of data flows that extend beyond international borders will be in the hundreds of billions of dollars in the year 2020, while the value of global data is in the trillions of dollars. By 2025, it is projected that the cumulative amount of data worldwide will exceed 175 zettabytes, with an estimated contribution to economic growth of $11 trillion [8].

However, the regulatory landscape for these data flows remains fragmented and underdeveloped. Despite the foundational role of the WTO in fostering global trade cooperation, its e-commerce negotiations have yet to yield a consensus on cross-border data flow governance, illustrating the challenges in forming multilateral rules in this domain. In contrast, regional cooperation has emerged as a more viable pathway for governing data flows, with the US and the EU leading the charge through agreements like the U.S.-Mexico-Canada Agreement and the U.S.-Japan Digital Trade Agreement. These efforts aim to streamline data governance on a regional scale but also highlight the fragmentation and inconsistency in global data governance approaches. This lack of a unified regulatory framework poses significant challenges for multinational corporations, complicating compliance and increasing the costs associated with policy adjustments.

Financial and Legal Challenges of Data Compliance in a Global Landscape.

The financial implications of data compliance present a formidable challenge for companies, particularly in the context of global operations where legal systems vary significantly. Recent research has found non-compliance can be up to 2.71 times higher than the cost of implementing compliant measures. Investing in data compliance is a necessary and wise business decision. To avoid potential legal, financial, and reputational damage, companies must prioritize compliance and allocate appropriate resources to ensure they adhere to data regulations [9]. Yet, the financial burden of achieving such compliance is notably steep, acting as a considerable barrier, especially for small businesses where the high costs may deter adherence to regulations, pushing them towards potentially risky practices.

The complexity of navigating through diverse and often conflicting data protection laws across different jurisdictions adds to the challenge. With laws and regulations continuously evolving to better protect consumer privacy, companies must remain vigilant and adaptable to stay compliant. This dynamic legal landscape, coupled with the novelty and rapid changes in privacy and data protection legislation, significantly increases the compliance costs for multinational corporations [10].

2.3 Technical and Managerial Compliance Challenges

Lack of Professionals in the Field.

There is a growing demand for experts who understand the technical and legal aspects of data compliance. Often called compliance officers, compliance professionals ensure that businesses remain updated on all regulatory and licensing obligations under the laws of the state, local, and federal governments. These experts create, put into practice, and uphold rules and procedures that ensure a business's goods, operations, and physical locations run morally and legally [11]. However, due to the novelty of the field of data compliance and the dramatic increase in demand, there is still a shortage of such skilled professionals.

Challenges of Internal Data Management.

Under the background of big data, the data generated in the process of production and operation of enterprises grows dramatically, in which multinational corporations have extensive business involving various countries, so the volume and variety of data of multinational corporations are huge and complex. Differences in norms for data management across sectors and regions also pose challenges for data integration.

The Importance of Compliance Culture and Employee Training.

A significant barrier to effective data governance is the lack of compliance risk awareness among business managers, who often fail to grasp the various categories of corporate governance risk fully. This gap in understanding leads to overlooking compliance risks, thereby amplifying the potential for data security breaches. Moreover, the casual approach of employees and their families towards online postings related to the enterprise can inadvertently create security vulnerabilities. These factors underscore the

need for enhancing compliance awareness throughout the organization and underscore the critical role of employee training in bolstering data privacy and security measures.

3 Case Study: Data Compliance in Multinational Corporations

3.1 Case Selection and Background

Selection Criteria for Case Companies.

In exploring the intricacies of data protection on a global scale, this study establishes three key criteria for selecting representative case companies. The primary focus is on multinational corporations, given their expansive operations across the globe and frequent encounters with cross-border personal information data scenarios, making them prime subjects for analysis. Secondly, the study narrows its focus to Internet enterprises, which are inherently more entangled in network security issues due to their digital nature. Finally, companies embroiled in disputes or litigation over cybersecurity compliance are chosen to elucidate the core challenges and strategies in this domain, as these situations provide concrete examples of the complexities involved in navigating cybersecurity compliance on an international level.

Cases.

TikTok, a video-sharing application developed by the technology company ByteDance, illustrates the first case. Despite utilizing the same software, TikTok and its Chinese counterpart, Douyin, operate on separate networks to adhere to China's censorship laws [12]. In 2023, this separation became a focal point of concern for lawmakers in the United States, Europe, and Canada, who intensified their efforts to restrict TikTok access due to perceived security threats [13]. Western regulators express apprehension that the Chinese government might leverage TikTok and ByteDance to amass extensive user data. In response, TikTok has assured that its user data is securely stored in data centers located in the US, Malaysia, and Singapore, with plans underway to establish a new center in Ireland.

The second case is a 2013 incident in which, as part of an investigation into drug trafficking, the US government demanded customer emails from Microsoft servers located in Ireland. Microsoft argued that US warrants did not apply to data stored outside of the country. This contention set the stage for the United States to formulate the Clarifying Lawful Overseas Use of Data (CLOUD) Act in 2018, a legislative milestone that addressed the complexities of retrieving data stored on overseas servers and underscored the evolving challenges in the intersection of international law and digital privacy [14].

3.2 Causes of the Problem

Legal and Policy Factors.

The legal and policy landscape surrounding data protection and cybersecurity is marked by rapid evolution and considerable diversity across jurisdictions. The enactment of the CLOUD Act in the United States, aimed at clarifying the legal framework for accessing data stored overseas, highlights the ongoing efforts to adapt legal systems to the realities of the digital age. However, this adaptation is not without its challenges. Jurisdictional uncertainties and conflicts with other countries' data sovereignty laws pose significant obstacles to seamless international operations. The Microsoft case, where a court ruled against the obligation to comply with a warrant for emails stored on foreign servers, underscores the inadequacies of outdated legal frameworks to address new technological contexts. Furthermore, geopolitical tensions, as evidenced in the U.S. government's scrutiny of TikTok, introduce additional layers of complexity, affecting not only legal compliance but also market access and operational stability for multinational tech companies.

Managerial and Technical Factors.

On the managerial and technical front, companies grapple with ensuring that their internal policies, processes, and systems align with an ever-expanding array of international legal requirements. TikTok's operation, heavily reliant on data-driven algorithms to curate user experiences, highlights the challenges of maintaining transparency and protecting user data rights. Its system tailors user experiences by analyzing various data points such as friends, geographic locations, and browsing histories to create detailed "data portraits," which are then used to fine-tune content delivery and meet users' information needs. An incident that underscores these challenges involved an anonymous former TikTok employee revealing to Washington Post reporters a code that allegedly linked TikTok with a China-based news app. According to the report, this code could potentially allow access to a backdoor into TikTok, enabling unauthorized interception of user data [15]. In response to such concerns, ByteDance has revamped its management team, emphasizing that TikTok's international operations are entirely managed by the US team to prevent unauthorized access to overseas data and code, reflecting a proactive approach to bolster data protection and comply with global standards.

3.3 Insights from the Current Situation Analysis

Recognition of Common Problems.

The United States extension of the jurisdiction of the Cloud Act extraterritorially does not constitute a flagrant violation of international law, but it is suspected of departing from the concept of data governance in the relevant international law documents. Three subjects were involved in this case, multinational corporations, Ireland, and the United States. According to the Irish Government, arbitrary access by the United States to data stored in its territory would jeopardize Ireland's national sovereignty and constitute interference with national sovereignty. The United States, on the other hand, overemphasizes data sovereignty. Transnational corporations are caught in

the middle of the law between the two countries. Initiatives on global data governance reforms are not coherent, with country-to-country systems in the global data domain being inadequate for deep-seated reasons rooted in culture and society. As a result, the complexity of the legal system and lack of international cooperation exposes multinational corporations to multiple compliance challenges.

Reflections.

Nowadays, the world has not yet reached a unified rule or consensus, and there are differences in the focus of different countries and concerns, for instance, the European Union prioritizes individual data control, while the United States emphasizes the advantages of data for businesses. China, on the other hand, emphasizes the integration of security and development, which imposes stricter demands on multinational companies to adhere to compliance systems at both the managerial and technical levels. Compliance with legal requirements shouldn't be the exclusive domain of multinational enterprises. The requirements of several dimensions, including politics, national security, the public interest, cultural traditions, and even customs, are also included in compliance. Multinationals should consider various factors in the compliance process as well as enhance compliance technology and improve management practices.

4 Strategies for Enhancing Data Compliance Globally

4.1 Legal and Policy Strategies

Promoting International Legal Standardization.

There is a growing number of international mechanisms related to cross-border data flows, but a harmonized and consensual core mechanism has yet to emerge. The inconsistency of laws and regulations between different countries and regions can be bridged by signing multilateral or regional data flow agreements and promoting international organizations to set data protection standards. Such agreements could serve as a foundational step towards creating a cohesive legal framework that aligns diverse international standards, providing clarity and predictability for multinational corporations. Furthermore, the role of international organizations in this context is indispensable. By spearheading initiatives to establish comprehensive data protection standards, these organizations can play a pivotal role in shaping a global consensus on key issues like personal data rights, data processing protocols, and security measures. Countries also need to develop regulations on personal data rights, data processing principles, data security requirements, etc. to adapt to the global.

Enhancing International Legal Cooperation.

The degree of restriction and the control of cross-border data flows differ significantly, even when the same trade agreement is signed and the advantages of cross-border data flows are acknowledged from an economic and social standpoint. This variability spans from the light-touch models adopted by countries like Australia, Canada, and Mexico, to the more restrictive approaches seen in China and Russia, which are

gaining traction in other developing nations [16]. Therefore, it is important to strengthen international cooperation and enhance the exchange of ideas on cross-border data transfer between countries. Nations can enhance legislative collaboration and provide a robust framework for the exchange of data across borders by creating rules and regulations that are mutually recognized. Cooperative mechanisms for offshore data access and retrieval need to be established so that national law enforcement agencies can legally access and retrieve cross-border data and so that States can work together to combat criminal and illegal activities in cross-border data flows. Moreover, there is a need to increase the exchange of information and sharing of experiences among countries to jointly address data flow and privacy protection issues. For example, promoting communication and cooperation among technicians from different countries as well as providing each other with national policy guidance and training on laws and regulations.

4.2 Internal Corporate Governance Strategy

Building a Data Protection Governance Framework.

The EU proposes a risk-based approach to protection through GDPR, urging companies to categorize data based on risk levels and implement corresponding protective measures. This necessitates regular impact assessments to ascertain the efficacy of these measures. To support this framework, it's recommended that companies establish a dedicated data compliance management department, equipped with adequate authority, resources, and funding. This department is tasked with formulating a comprehensive data compliance strategy, enhancing the compliance program, ensuring alignment with data regulations across business operations, and devising strategies to mitigate data risks. A multidisciplinary team comprising legal, IT, and operational experts is essential for this department, especially for multinational corporations operating across various jurisdictions. This setup not only facilitates compliance with local data regulations but also aids in streamlining compliance costs and refining business processes through the accumulation of diverse regional data transaction experiences.

Enhancing Internal Compliance Culture and Awareness.

Enterprises can help their employees understand the information protection concepts and codes of conduct involved in their business through knowledge training and daily communication, as well as consultation and advice. They can also regularly review the compliance of internal operations with information protection management standards, set up hotlines to receive reports of violations, and provide advice and guidelines on handling procedures when necessary. Enterprises can incorporate data security and compliance into employee performance appraisal management, rewarding those with positive data compliance awareness and behavioral compliance, and punishing those involved in data security breaches, to ensure the establishment of the enterprise's data compliance management system.

4.3 Technology Solutions Strategy

Advanced Data Protection Technologies.

Encouraging and supporting innovation in cross-border data flow governance technology is crucial, including data encryption technology, privacy protection technology, secure transmission technology, etc., to raise the standard and capacity of technological cross-border data governance. To guarantee that the development of cross-border data governance capacity keeps up with technical innovation, the system of oversight for the flow of data across borders is periodically adjusted while staying up to date with the most recent trends in technology development.

Advanced data protection techniques, such as encryption, two-factor authentication, and regular security updates, can aid in guarding against potential data breaches and preventing unauthorized access to sensitive data.

Data Minimization and Data Anonymization.

When collecting information data, companies and governments should abide by the data minimization principle. The General Data Protection Regulation (GDPR) stipulates that personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed (data minimization) [17], which means that the data controller must assess whether the purpose can be achieved by processing anonymized data with all unique identifiers removed. The amount of personal data processed is limited to the minimum necessary to meet the needs of the business and no non-essential personal data may be collected. This not only helps to reduce the workload of data protection but also better protects the security of data information. Implementing data minimization properly can benefit enterprises or governments in several ways, including enhancing compliance, decreasing the impact of leakage, minimizing risk, and decreasing storage expenses.

However, after data collection, how to ensure the security of data is a universal problem faced by enterprises and government. To ensure the confidentiality of sensitive or private information, data anonymization involves the erasure or encryption of identifiers that link a specific individual to the data that is stored [18]. Data anonymization includes data masking, pseudonymization, data aggregation, data randomization, data generalization, and data swapping. A lot of data security legislations (like APPI, CPRA, GDPR, and HIPAA) set out that companies should take precautions to protect confidential data. Through data anonymization, enterprises can enhance data security and minimize the risk of data breaches when obscuring or removing data information from a dataset. Furthermore, it aids in cost reduction by allowing for the reuse of data without requiring consent and eliminating the requirement for safe storage. These factors contribute to the overall reduction of expenses related to data management and analytics.

5 Conclusion

In conclusion, this paper analyzes and discusses multinational companies' cybersecurity compliance challenges and strategies from three perspectives: the difficulties of data protection, relevant cases, and solution strategies. This paper has generally found that the diversity of global legal standards, different positions in government and enterprises, and technical and managerial challenges are the main causes of the difficulties in data compliance. These findings have provided a deeper insight into the importance of data security and how to improve data compliance by tackling the existing problem.

For multinational companies, it's difficult to improve the global legal environment on data security, therefore, building a strong data protection framework to enhance internal compliance standards, improving compliance culture, and employee awareness within the company, and updating cutting-edge data protection technology is the first step multinationals should take if emphasizing data compliance as important.

In the era of the digital economy, countries attach great importance to data resources and regard them as the key to obtaining strategic competitive advantages in all facets of the economy, science and technology, security, and so on. The disorderly cross-border flow of data poses risks and damages to the interests of individuals, enterprises, society, and the state. This article may provide a basic compliance system for multinational corporations.

However, this study may be limited by the absence of harmonized international legal standards on data security. There are still no uniform standards for the application of laws in different regions or countries. States should strengthen international cooperation and coordination to tackle data protection challenges jointly because effective global data governance helps individuals to utilize and protect their data, and facilitates the development of transnational corporations while safeguarding national sovereignty.

References

1. Sun Y, Zhang J, Xiong Y, Zhu G. Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks. 2014;10(7). doi:10.1155/2014/190903Author, F., Author, S.: Title of a proceedings paper. In: Editor, F., Editor, S. (eds.) CONFERENCE 2016, LNCS, vol. 9999, pp. 1–13. Springer, Heidelberg (2016).
2. Aptum Homepage, https://aptum.com/knowledge-center/enterprise-data-security/,last accessed 2024
3. LNCS Homepage, http://www.springer.com/lncs, last accessed 2016/11/21.
4. While this is the understood meaning, detailed definitions of data security are rare, despite the prevalence of state data security laws. John Black, Developments in Data Security Breach Liability, 69 BUS. LAW. 199, 206 (2013).
5. Aosphere,Data Privacy - China's Personal Information Protection Law enters into force, October 28,2021,Retrieved on March 20,2024.Retrieved from: https:/ /www. aosphere. com/ aos/news-knowhow/data-privacy-china-pipl-enters-into-force.
6. United Nations Capital Development Fund, "The Role of Cross-Border Data Flows in the Digital Economy," July 2022, p. 1,Retrieved from: https: // static1. squarespace. com/ static/ 5f2d7a54b7f75718fa4d2eef/t/62ed6b995307db59e3e5d2c6/1659726787042.

7. McKinsey & Company, “Digital Globalization: The New Era of Global Flows,” March 2016, p. 75, Retrieved from: https://www.mckinsey.com/capabilities/ mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows.
8. Wendy Li, “Economic Values of Data and Data Flows, and Global Minimum Tax,” p. 1.
9. Meeba Gracyan, What Is Data Compliance And How Do We Implement It? January 4,2024
10. Chris Brook,Fortra.What Is Data Compliance? Top Regulations You Need to Know. February 21, 2024.Retrieved on March 24, 2024.Retrieved from:https://www.digitalguardian.com/blog/what-data-compliance-top-regulations-you-need-know#:~: text= Data% 20compliance%20has%20many%20advantages%2C%20but%20implementing%20it,storing%20more%20information%20than%20ever.%20...%20More%20items.
11. Shayna Joubert. Northeastern graduate. Compliance Specialists: Who They Are and What They Earn. March 29, 2018.Retrieved on 24 March, 2024.Retrieved from:https://graduate.northeastern.edu/resources/compliance-specialist-career-overview/.
12. Kaspersky, TikTok privacy and security - Is TikTok safe to use? Retrieved on March 27,2024, Retrieved from: https://usa.kaspersky.com/resource-center/preemptive-safety/is-tiktok-safe.
13. Sapna Maheshwari and Amanda Holpuch,The New York Times, Why the U.S. Is Weighing Whether to Ban TikTok. March 12, 2024.Retrieved on March 27, 2024.Retrieved from: https://www.nytimes.com/article/tiktok-ban.html.
14. Kiteworks | Demystifying the US CLOUD Act. Retrieved from: https://www.kiteworks.com/ risk-compliance-glossary/us-cloud-act/.
15. Scott Ikeda. Former TikTok Employee Claims User Data Still Leaking to China, Company Was “Intentionally Lying” to US Regulators [EB/OL].(2023-3-20). Retrieved from: https://www.cpomagazine.com/data-privacy/former-tiktok-employee-claims-user-data-still-leaking-to-china-company-was-intentionally-lying-to-us-regulators/.
16. UNCTAD, Digital Economy Report 2021, Cross-border data flows and development: For whom the data flow, September 29,2021,p.137.
17. GDPR. Art. 5. 1.(c).
18. Imperva. Anonymization. Retrieved from:https://www.imperva.com/learn/data-security/anonymization/#:~:text=Data%20anonymization%20is%20the%20process,an%20individual%20to%20stored%20data.Retrieved on April 2,2024.