DOI URL:https://doi.org/10.63944/2q3JFEMR

Vol.1 No.1

Research on Data Security and Privacy Protection in Corporate Human Resource Management in the Digital Era

Biao Zhang [1 2 *], Zhuoxin Li [1], Ke Xie [1], Ting Li [2], Binbin Huang [2]

[1] Guangzhou College of Technology and Business, Guangzhou, Guangdong, 510000

[2] Shenzhen Sijiu Consulting Co.,Ltd. Shenzhen, Guangdong, 518000

[*] Corresponding Author: Biao Zhang | zhangbiao@gzgs.edu.cn

Abstract: Against the backdrop of the global digital wave, human resource management (HRM) in innovation and entrepreneurship enterprises is undergoing profound transformation, with data emerging as a core asset driving corporate decision-making and development. However, issues related to data security and privacy protection have become increasingly prominent, serving as key factors restricting the sustainable development of enterprises. By analyzing the challenges faced by innovation and entrepreneurship enterprises in data security and privacy protection within HRM, this paper explores the importance of these issues and proposes countermeasures such as constructing a data security governance system, applying privacy computing technologies, and enhancing employees' data security awareness. The aim is to provide theoretical references and practical guidance on data security and privacy protection for innovation and entrepreneurship enterprises, helping them achieve a balance between security and development during digital transformation.

Keywords: Digital Era; Data Security; Privacy Protection

Funding Project: This paper is a phased achievement of the horizontal research project of Guangzhou College of Technology and Business entitled College Students' Entrepreneurial Intention and Realization Path under the Background of Artificial Intelligence (Project No.: KYHX2025032).

1. Introduction

With the rapid development of information technology, the digital era has arrived. Emerging technologies such as big data, cloud computing, and artificial intelligence continue to emerge and are widely applied in various fields, profoundly transforming the operation models and management methods of enterprises. In the field of innovation and entrepreneurship, to stand out in the fierce market competition, enterprises attach greater importance to the digital transformation of human resource management (HRM), realizing data-driven precision in talent recruitment, training and development, and performance management. However, while enjoying the convenience and efficiency brought by digitalization, issues of data security and privacy protection have become increasingly prominent.

In recent years, frequent data leakage incidents have caused huge losses to enterprises and individuals. For enterprises, data security and privacy protection are even related to their survival. Once a data leakage incident occurs, it may lead to serious consequences such as customer loss, declining investor confidence, and business interruption, and may even push the enterprise into bankruptcy. Therefore, researching data security and privacy protection in corporate HRM in the digital era holds significant practical significance.

2. Literature Review

Scholars at home and abroad have conducted extensive research on data security and privacy protection in corporate HRM in the digital era. Foreign scholars paid attention to the importance of data security and privacy protection relatively early, with relevant studies focusing on laws and regulations, technical means, and management strategies. For example, the European Union's General Data Protection Regulation (GDPR) sets strict provisions on the collection, storage, use, and sharing of personal data, providing a legal basis and normative standards for corporate data security and privacy protection. Domestic scholars, combining China's national conditions and corporate realities, have conducted in-depth research on data security and privacy protection. Some scholars propose that enterprises should establish and improve a data security governance system, strengthen data classification and risk assessment, and adopt advanced technical means and management measures to ensure data security and privacy protection. At the same time, other scholars emphasize the importance of cultivating employees' data security awareness, believing that employees are the first line of defense for corporate data security, and only by improving employees' data security awareness can the risk of data leakage be fundamentally reduced.

However, existing studies still have some shortcomings. On the one hand, there is relatively little research on [innovative entrepreneurial enterprises]—a specific group. These enterprises differ greatly from traditional enterprises in terms of scale, resources, and management, and their data security and privacy protection issues also have uniqueness. On the other hand, most existing studies focus on theoretical discussions, lacking in-depth analysis of practical cases and operable suggestions, making it difficult to meet the actual needs of enterprises. Therefore, this paper will focus on data security and privacy protection in corporate HRM in the digital era, and propose targeted countermeasures combined with practical cases.

Some scholars have explored the innovation of corporate human resource management in the context of the big data era, providing a certain theoretical basis for the digital transformation of HRM, which also indirectly highlights the urgency of data security and privacy protection in the process of HRM digitalization [1]. In terms of technical research, relevant studies on key technologies of deep learning data security and privacy protection have laid a technical foundation for solving data security problems in HRM [2]. From a legal perspective, research on corporate compliance focusing on privacy protection and data security has provided a legal reference for enterprises to deal with data security and privacy protection issues [3].

3. Challenges of Data Security and Privacy Protection in Corporate HRM in the Digital Era

3.1. Technical Level

In the digital era, enterprises widely apply various emerging technologies in HRM, such as big data analysis and artificial intelligence. However, the application of these technologies also brings new data security risks. On the one hand, data encryption technology has limitations. Although data encryption is a basic means of protecting data security, existing encryption algorithms may be threatened by new technologies such as quantum computing. Once the encryption algorithm is cracked, data will face the risk of leakage. On the other hand, network security protection technologies face challenges. With the continuous upgrading of hacker attack methods, traditional network security protection technologies such as firewalls and intrusion detection systems are difficult to effectively resist complex attacks like Advanced Persistent Threats (APT).

3.2. Management Level

In HRM, the imperfect data security management system is a prominent problem for enterprises. Many enterprises lack a clear data security management responsibility system, and the responsibilities of various departments in data security management are not clear, leading to loopholes in data security management. At the same time, data access control is not strict—employees can arbitrarily access and download sensitive data, increasing the risk of data leakage. In addition, the incomplete data backup and recovery mechanism is another major hidden danger. Some enterprises do not back up data regularly, or store backup data in unreliable locations. Once a data loss or damage incident occurs, data cannot be recovered in a timely manner, affecting the normal operation of the enterprise.

3.3. Legal Level

As data security and privacy protection issues become increasingly prominent, countries around the world have introduced relevant laws and regulations for regulation. However, for enterprises, there are certain difficulties in adapting to and complying with these laws and regulations. On the one hand, laws and regulations are updated rapidly, and enterprises find it difficult to timely understand and master the latest legal requirements, leading to potential violations of laws and regulations during data processing. On the other hand, laws and regulations vary across countries and regions. For enterprises operating internationally, they need to comply with the laws and regulations of multiple countries and regions simultaneously, increasing the cost and difficulty of compliance.

To further clarify China's compliance requirements, the mapping relationship between core compliance clauses at home and abroad is supplemented below, helping enterprises accurately align with domestic and foreign legal norms:

Table 1. Mapping Table of Core Compliance Clauses for Data Security and Privacy Protection at Home and Abroad

Compliance Dimension	Requirements of Relevant Chinese Laws (Personal Information Protection Law, Data Security Law, Cyber Security Law and supporting norms in the human resources field)	EU GDPR Requirements
Minimization of Collection	The collection of personal information shall be limited to the minimum scope necessary to achieve the processing purpose, and excessive collection shall be prohibited; the collection of employee information in human resource management shall be directly related to specific purposes such as employment management and salary and welfare, and irrelevant information shall not be collected	The collection of personal data shall be lawful, fair and transparent, and limited to specific, clear and lawful purposes, and shall not be collected beyond the necessary scope
Informed Consent	Before collecting employees' personal information, it is necessary to inform the purpose, scope and other matters of collection and use in a prominent manner and in clear and understandable language, and obtain the explicit consent of employees; consent can be withdrawn, and relevant information shall not be processed continuously after withdrawal	Data subjects have the right to obtain transparent information notification, and data processing shall be based on the explicit consent of data subjects, which shall be specific, free and revocable
Purpose Limitation	The processing of employee data shall be consistent with the informed purpose; if the purpose needs to be changed, it is necessary to inform again and obtain consent; the employee data collected in human resource management shall not be used in irrelevant business scenarios	The purpose of data processing shall be determined at the time of collection and shall not be contrary to the original purpose; if the purpose needs to be changed, it is necessary to ensure that the new purpose is compatible with the original purpose and inform the data subject
Cross-border Rules	If employee data needs to be transmitted across borders, it is necessary to meet compliance conditions such as security assessment, standard contracts and certification, and inform employees of matters such as the recipient and purpose of cross-border transmission to protect employees' right to know	The transfer of data to a third country or international organization shall meet conditions such as adequacy determination and appropriate safeguards (such as standard contracts, binding corporate rules) to ensure the security of data during cross-border transmission
Limitations on Employee Profiling	It is prohibited to use employee data for unreasonable profiling analysis, such as discriminatory treatment of employees based on profiling (in terms of salary, promotion, etc.); the results of profiling shall be explained to employees to protect their right to know and right to object	Data subjects have the right to object to decisions made based on automated processing (including profiling) that have legal effects or similar significant effects on them, and enterprises shall provide the right to human intervention, express opinions and raise objections

3.4. Personnel Level

Employees’ weak data security awareness is another important challenge for corporate data security and privacy protection. Some employees have insufficient understanding of the importance of data security, lack basic data security knowledge and skills, and are prone to data leakage behaviors in daily work. For example, employees may log in to the enterprise system using unsafe devices in a public network environment, or arbitrarily send sensitive data to others. In addition, insufficient employee training is also one of the reasons for weak data security awareness. Many enterprises do not regularly organize data security training for employees, or the training content lacks targeting and practicality, making it impossible to effectively improve employees’ data security awareness and skill levels.

4. Importance of Data Security and Privacy Protection in Corporate HRM in the Digital Era

4.1. Safeguarding Corporate Core Competitiveness

Data is one of the core assets of an enterprise, including important content such as corporate trade secrets, customer information, and technical solutions. Protecting data security and privacy can prevent competitors from obtaining the enterprise's core data, avoid the leakage of corporate trade secrets, and thus safeguard the enterprise's core competitiveness. Therefore, strengthening data security and privacy protection is crucial for maintaining the enterprise's core competitiveness.

4.2. Maintaining Corporate Reputation and Customer Trust

In the digital era, customers are paying more and more attention to enterprises' data security and privacy protection capabilities. Once a data leakage incident occurs in an enterprise, it will seriously damage the enterprise's reputation and customer trust. Customers may worry about the leakage of their personal information, thereby reducing cooperation with the enterprise or turning to other enterprises. Conversely, if an enterprise can strengthen data security and privacy protection and demonstrate its reliable data management capabilities to customers, it will help improve the enterprise's reputation and customer trust, and promote the long-term development of the enterprise.

4.3. Complying with Legal and Regulatory Requirements

With the continuous improvement of data security and privacy protection laws and regulations, enterprises must comply with relevant laws and regulations to ensure the legality and compliance of data processing activities. Otherwise, enterprises will face risks such as huge fines and legal lawsuits, and may even lead to bankruptcy. For example, the EU's GDPR stipulates that enterprises violating data protection regulations may be fined up to 4% of their global annual turnover ; China's Personal Information Protection Law also clearly stipulates that enterprises that illegally process personal information in serious cases may be fined up to 500 million yuan or 5% of the previous year's turnover. Therefore, strengthening data security and privacy protection is an inevitable requirement for enterprises to comply with laws and regulations and avoid legal risks.

4.4. Promoting Sustainable Corporate Development

In the digital era, data security and privacy protection are important guarantees for the sustainable development of enterprises. A stable data security environment can provide a good development foundation for enterprises, enabling them to focus on business innovation and development. At the same time, strengthening data security and privacy protection also helps enterprises attract and retain outstanding talents, and improve employees' loyalty and work enthusiasm. For state-owned enterprises, the innovation of human resource management under the background of the knowledge economy era also needs to take data security and privacy protection as an important support to promote the sustainable development of enterprises.

5. Countermeasures for Data Security and Privacy Protection in Corporate HRM in the Digital Era

5.1. Establishing a Data Security Governance System

Enterprises should establish and improve a data security governance system, clarifying the goals, principles, and processes of data security management. Set up a dedicated data security management institution responsible for the overall planning and coordination of data security management. Formulate a data security management responsibility system, clarify the responsibilities and authorities of various departments and employees in data security management, and ensure that data security management work is implemented effectively.

5.2. Strengthening Data Classification and Risk Assessment

Classify the data in HRM to clarify the sensitivity and importance of different types of data. Based on the results of data classification, formulate corresponding protection measures. For example, classify sensitive data such as employees' personal information and salary data as high-level protected data, and adopt strict protection measures such as encrypted storage and access control; classify general business data as low-level protected data, and adopt relatively loose protection measures. At the same time, conduct regular data security risk assessments to identify potential data security risks and formulate risk response strategies.

5.3. Applying Privacy-Enhancing Technologies (PETs)

To achieve the accurate alignment between technical paths and compliance obligations, the application of privacy-enhancing technologies and corresponding compliance requirements are clarified as follows:

Secure Multi-Party Computation: In the recruitment process of human resources, enterprises can cooperate with multiple recruitment platforms through secure multi-party computation technology to conduct a comprehensive evaluation of candidates' resumes without disclosing candidates' personal information (such as education background and work experience). The application of this technology complies with the compliance requirements of "minimization of collection" and "purpose limitation"—only the necessary information for evaluation is obtained, and the data use is strictly limited to the recruitment and screening scenario, avoiding excessive collection and abuse of information.

Federated Learning: In the link of employee training and development, enterprises can cooperate with other enterprises or training institutions through federated learning technology to jointly develop training courses and optimize training programs without sharing the learning data of employees from all parties (such as learning progress and weak knowledge points), so as to provide personalized training for employees. The application of this technology meets the compliance requirements of "informed consent" and "limitations on employee profiling"—it is necessary to inform employees of the purpose of using data for joint modeling in advance and obtain consent, and avoid unreasonable profiling and discriminatory training arrangements based on employees' learning data during the modeling process.

Privacy-enhancing technologies (such as secure multi-party computation and federated learning) can realize data sharing and value mining without leaking raw data. Enterprises can apply these technologies to HRM to make full use of data for HRM decision-making while ensuring data security and privacy. Relevant research on key technologies of deep learning data security and privacy protection can provide technical support for the application of these technologies .

5.4. Improving Employees' Data Security Awareness

Strengthen data security training for employees to improve their data security awareness and skill levels. The training content should include data security laws and regulations (such as Personal Information Protection Law, Data Security Law, Cyber Security Law), corporate data security management systems, data security operating procedures, common data security threats, and prevention methods. Through regular training and assessments, ensure that employees master the necessary data security knowledge and skills.

5.5. Improving Data Backup and Recovery Mechanisms

To strengthen the connection between technical measures and compliance obligations, the compliance requirements corresponding to the data backup and recovery mechanism are supplemented here:

Establish a regular data backup system, clarify the backup frequency (such as daily incremental backup and weekly full backup) and backup content (covering core human resource data such as employees' personal information, salary data, and performance records) to ensure the timely backup of important data; select reliable backup storage media and locations (such as adopting a combination of local backup and remote disaster recovery) to avoid the loss or damage of backup data. At the same time, formulate a data recovery plan, clarify the data recovery process, responsible persons, and recovery time limit, and conduct regular data recovery drills to ensure that data can be recovered quickly and effectively in case of data loss or damage. The construction of this mechanism complies with the compliance requirements of "ensuring data integrity and availability" in the Data Security Law and the obligation of "taking necessary measures to ensure the security of personal information" in the Personal Information Protection Law, avoiding the impact on enterprise operations and employee information security due to data loss.

5.6. Strengthening Compliance Management

Pay close attention to the updates and changes of domestic and foreign data security and privacy protection laws and regulations (such as the special norms for human resource data management issued in China's human resources field and the revision trends of EU GDPR), and adjust the enterprise's data processing activities in a timely manner to ensure compliance with legal and regulatory requirements. Establish a compliance management mechanism to conduct regular reviews and assessments of the enterprise's data processing activities, and identify and correct non-compliant behaviors. At the same time, external compliance consulting institutions can be introduced to assist enterprises in conducting compliance self-inspections and risk investigations, and improve the level of compliance management. Research on corporate compliance from a legal perspective can provide a reference for enterprises to strengthen compliance management .

6. Conclusions and Prospects

6.1. Research Conclusions

The digital era brings new opportunities and challenges to corporate HRM, and data security and privacy protection have become important factors restricting corporate development. By analyzing the challenges faced by data security and privacy protection in corporate HRM—such as limitations of data encryption technology and challenges to network security protection technologies at the technical level; imperfect data security management systems and lax data access control at the management level; difficulties in adapting to and complying with laws and regulations at the legal level; and employees' weak data security awareness at the personnel level—this paper emphasizes the importance of data security and privacy protection in safeguarding corporate core competitiveness, maintaining corporate reputation and customer trust, complying with legal and regulatory requirements, and promoting sustainable corporate development.

In response to these challenges and issues, this paper proposes countermeasures such as establishing a data security governance system, strengthening data classification and risk assessment, applying privacy-enhancing technologies, improving employees' data security awareness, improving data backup and recovery mechanisms, and strengthening compliance management. These strategies aim to provide theoretical references and practical guidance for enterprises in data security and privacy protection, helping enterprises achieve a balance between security and development in the process of digital transformation. The innovation of corporate human resource management in the big data era also needs to be supported by these countermeasures to ensure the smooth progress of digital transformation [4].

6.2. Research Prospects

In the future, with the continuous development and innovation of digital technologies, data security and privacy protection in corporate HRM will face more challenges and opportunities. On the one hand, emerging technologies such as blockchain and quantum computing will bring new solutions to data security and privacy protection. For example, blockchain technology has the characteristics of decentralization and immutability, which can be applied to the secure storage and sharing of data to improve data security and credibility; if quantum computing technology can make a breakthrough, it may greatly improve the strength of data encryption and resist attacks that are difficult to deal with by existing technologies. On the other hand, laws and regulations will continue to improve, and requirements for corporate data security and privacy protection will become more stringent. Enterprises need to continuously strengthen their own data security and privacy protection capabilities to adapt to changes in laws and regulations.

Future research can further explore the application of emerging technologies in data security and privacy protection of corporate HRM, and how to establish a more complete legal and regulatory system to protect the data security and privacy rights of enterprises and individuals. At the same time, practical case studies can be carried out to summarize the successful experiences and failure lessons of enterprises in different industries and of different scales in data security and privacy protection, providing more targeted references for other enterprises. For state-owned enterprises, in the process of human resource management innovation under the background of the knowledge economy era, the research on data security and privacy protection also needs to be further deepened [5].

References

[1] Song, H. (2021). Thoughts on the Innovation of Corporate Human Resource Management in the Big Data Era. Talent Resource Development, (07), 95-96.
https://doi.org/10.19424/j.cnki.41-1372/d.2021.07.040

[2] Tang, F. Y. (2021). Research on Key Technologies of Deep Learning Data Security and Privacy Protection (Master's Thesis). National University of Defense Technology. https://doi.org/10.27052/d.cnki.gzjgu.2021.000072

[3] Cheng, Y. (2025). The Key to Corporate Compliance in the Digital Era: Privacy Protection and Data Security from a Legal Perspective. Legal Expo, (03), 163-165.

[4] Song, L. J., & Yuan, L. (2020). Thoughts on the Innovation of Corporate Human Resource Management in the Big Data Era. Management & Technology of SME, (11), 66-67.

[5] Guo, Y. Y. (2024). Thoughts on the Innovation of Human Resource Management in State-Owned Enterprises under the Background of the Knowledge Economy Era. Market Outlook, (17), 190-192.