Study on Legal Risks and Management Strategies of Data Application Based on Customer Data Protection

Jiayun Shi

Researcher of State Grid Energy Research Institute

shijiayun@sgeri.sgcc.com.cn

Abstract. This paper is based on the legal provisions of personal data protection and analyzes the possible legal risks in the use of customer data and corresponding management strategies. The paper analyzes the cases of customer data privacy protection in China and abroad, and draws on the experience of typical enterprises in protecting customer data privacy. Based on practice, the paper analyzes the risks of data application in key areas such as collection, retention, use, and circulation, and proposes corresponding prevention methods and management strategies.

Keywords: Personal data protection; Data management; Risk prevention; Digital economy

1 Introduction

The value of data ownership has long been recognized, and the application and management of data are issues of property rights allocation in economics. [1] With the development of the digital economy, more and more theories have been proposed to allocate data resources, such as data production theory. [2] Resource allocation cannot be separated from legal regulation. Globally, legislation and enforcement on personal data protection are becoming increasingly stringent. The European Union (EU) has the most comprehensive legislation on personal data protection, and the introduction of the EU General Data Protection Regulation has sparked a wave of research on personal data protection. Related studies mainly focus on the nature of EU personal data rights [3] and the circulation of data within the EU. [4] At the same time, many scholars are concerned about the balance between EU personal data protection and commercial use. [5] With the introduction of China's Personal Information Protection Law, research on personal data protection in China has also become a hot topic. Current research mainly explains why personal data should be protected from a theoretical perspective [6], and emphasizes the dual interests of personality and property in personal data [7][8][9]. There are few articles exploring how to regulate the use of personal data from a corporate perspective, and they mainly focus on the protection and management of data in the financial industry. [10][11] There are few articles that provide risk warnings and management suggestions for each stage of the entire lifecycle of personal data used for

L. Moutinho et al. (eds.), *Proceedings of the 2023 International Conference on Management Innovation and Economy Development (MIED 2023)*, Advances in Economics, Business and Management Research 260,
https://doi.org/10.2991/978-94-6463-260-6_56

commercial purposes from the perspective of customer personal data. This paper starts with legal and compliant methods to unleash the value of data and stimulate the vitality of the data economy, proposes risks and prevention and management strategies for several stages of customer data application, and explores ways to legally and fully protect customer personal data within the current legal framework, providing a solid guarantee for promoting the better development of the digital economy.

2 Legislation and Case Analysis of Personal Data Protection in China and Abroad

2.1 Research on Legislation of Personal Data Protection in China and Abroad

2.1.1 Legislation in China.

Currently, the framework for personal data protection legislation has been preliminarily established in China.（as shown in Figure 1) According to the Personal Information Protection Law formulated in accordance with the Constitution of the People's Republic of China, the rights of the subjects of personal information are protected as basic rights of citizens.[1] In addition, relevant provisions on personal information protection are included in laws, administrative regulations such as the Civil Code of the People's Republic of China, the Criminal Law of the People's Republic of China, and the Law of the People's Republic of China on the Protection of Consumer Rights and Interests.

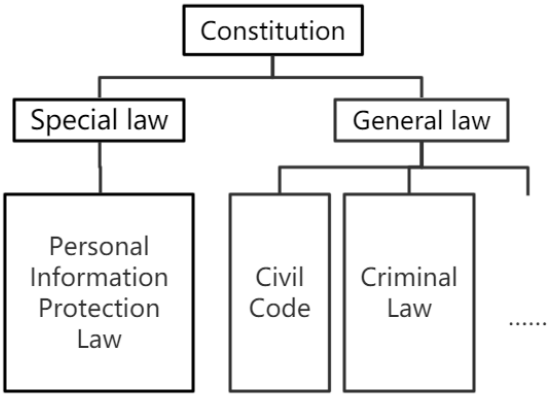

Fig. 1. Framework for personal data protection legislation in China

[1] Article 1 of the Personal Information Protection Law: "In order to protect the rights and interests of personal information, regulate the processing of personal information activities, and promote the rational use of personal information, this law is formulated in accordance with the Constitution."

2.1.2 Legislation Abroad.

Personal data protection legislation is increasingly valued worldwide, and its content is constantly enriched.

The General Data Protection Regulation enacted by the European Union in 2018 comprehensively regulates all aspects of personal data protection based on the characteristics of the big data era. It stipulates many rights of personal data subjects, proposes several principles that must be followed in processing personal information, and establishes strict protection principles, regulatory methods, and punishment mechanisms.

The United States focuses on the regulatory role of the market in personal data protection, while limiting government intervention as much as possible. Therefore, the laws related to personal data protection in the United States have a fragmented feature, and there is no unified personal data protection legislation, but there are hundreds of federal and state laws related to personal data protection.

2.2 Case studies on personal data protection in China and abroad

2.2.1 Case studies on personal data protection in China.

Based on the analysis of cases such as the privacy disputes between Zhao Peng and Yang Xidong, the infringement liability disputes between Shen Jin and Alipay Network Technology Co., Ltd., and the privacy disputes between Li Libin and the China Insurance Regulatory Commission, the following conclusions related to enterprise management can be drawn:

- The disputed behaviors involved in the cases cover the entire process of personal information collection, storage, and use throughout its lifecycle.
- Among them, the three types of behaviors involving "personal information recording errors," "unauthorized use of personal information," and "personal information leakage" have the highest number of cases.
- Many cases reflect disputes over the business model of personal information collection and use.
- The types of liability for personal information infringement include apologizing and compensating for economic losses, which may damage the company's reputation and cause economic losses, and should be prevented.
- The construction of the company's personal data management system and specific measures are highlighted in the determination of fault in specific cases.

2.2.2 Case studies on personal data protection abroad.

In 2015, Facebook used facial recognition technology in its photo tagging feature, which allowed users to tag friends in photos uploaded to Facebook and create links to their friends' profiles. However, the platform scanned users' uploaded facial images without their consent, violating Illinois' Biometric Information Privacy Act. As a result, representatives of 1.6 million affected users filed a class-action lawsuit.

In 2020, video conferencing software company Zoom reached a settlement with the U.S. Federal Trade Commission over privacy infringement issues. In the allegations, the U.S. Federal Trade Commission claimed that Zoom had misled consumers since at

least 2016, promising data encryption levels that the company did not provide in the past four years.

These two cases not only brought huge fines to the companies but also had a negative impact on their image.

3 Main practices and references of typical companies in personal data protection

3.1 Google: Advanced practices in protecting customer privacy

Google's protection of customer data mainly involves three levels: personnel, management, and technology. At the personnel level, Google has built an inclusive security culture for employees, established a dedicated operations team, and improved restriction and incentive mechanisms for internal employees and external researchers. In terms of management, Google mainly follows GDPR to carry out data management and proposes a "four-step approach" to respond to data events based on it. At the technical level, Google builds cloud infrastructure with security at its core to ensure data security throughout its lifecycle.

3.2 Huawei Cloud: System construction and specific measures for data protection

Huawei Cloud has established a complete set of data and privacy protection systems to lay a solid foundation for the company's subsequent development and application of specific data protection measures. In addition, the construction of data protection processes covering various businesses is conducive to standardizing data protection work, making customers more confident in the company's data processing behavior when using related services. The various qualifications and industry standard recognitions obtained by the company are also one of the key manifestations of the company's data compliance measures.

3.3 Trends and Conclusions Shown in Relevant Management Cases

Current practices related to enterprise data protection can be summarized as follows: First, establish and improve data privacy protection policies and systems; Second, use various technical and management measures to improve the hierarchical protection of various types of data, especially personal information; Third, enterprises should fully leverage their advantages in independent innovation in data protection, research and develop advanced data compliance tools, and apply them; Fourth, actively obtain recognition of various data protection capabilities.

4 Potential Risk Analysis of Personal Data in Business Applications at Each Stage

Analyzing the potential risks of personal data at each stage of business application is helpful for proposing corresponding prevention measures and management strategies. (Figure 2)

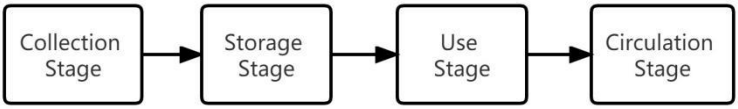

Fig. 2. Each stage of business application of personal data

4.1 Risk in Collection Stage

First, failure to obtain informed consent for processing personal information. Second, collecting personal information beyond the actual usage purpose, mainly manifested in collecting unnecessary personal sensitive information.

4.2 Risk in Storage Stage

First, storing personal information beyond the necessary retention period, such as failing to establish clear mechanisms for expiration deletion or anonymization of collected information. Second, inadequate self-obligation management. Third, failure to separate and manage test data properly.

4.3 Risk in Use Stage

First, insufficient data tracing in the use stage. Second, insufficient data desensitization during the data use process. Third, unauthorized use of personal data beyond the authorized scope in the agreement, and failure to obtain new informed consent when increasing the operations of personal data processing. Fourth, failure to explicitly inform users of using personal data for personalized decision-making.

4.4 Risk in Circulation Stage

First, desensitization processing of data before external sharing. Real data is not static, it changes with time, and the scale of data also changes constantly. It is difficult to accurately evaluate the risk of sensitive information leakage in data sharing, making it difficult to achieve fully effective desensitization processing of data, which poses a risk of sensitive information leakage. Second, lack of data security guarantees for the interaction channels of third-party units. Third, lack of supervision over data security protection for external interaction interfaces.

5 Research on Personal Data Risk Prevention and Management Strategies

5.1 Research on Risk Prevention and Management Strategies in the Collection Stage

When collecting information, companies should follow the principles of informed consent and minimal necessary, and in practical terms, companies should update privacy policies in a timely manner, ensure that the collection content is minimal and necessary, and fully fulfill their disclosure obligations.

5.2 Research on Risk Prevention and Management Strategies in the Storage Stage

First, pay attention to the classification and partitioned storage of data. Classifying and saving personal data is an important privacy risk prevention strategy. Personal privacy infringement often involves personal sensitive information, so it is crucial to identify and protect personal sensitive information. Second, improve the notification system for data leaks. Once a situation involving the leakage of user privacy is discovered, the company has an obligation to promptly stop it to avoid the expansion of losses. Third, establish a reasonable data deletion system, immediately delete relevant data that exceeds the retention period specified during the collection stage, and use various deletion methods.

5.3 Study of Risk Prevention and Management Strategies in the Use Stage

First, establish the principle of legitimacy in data use based on the requirements of national laws and regulations for the protection of personal information and important data, and clarify the purpose and scope of data use and analysis. Second, establish an internal accountability system for data use to ensure the use and analysis of protected data within the declared purpose and scope of data use. Third, follow the principle of least privilege and provide a fine-grained access control mechanism to limit the scope of data accessible and the purpose of its use during the data use process.

5.4 Study of Risk Prevention and Management Strategies in the Circulation Stage

Personal data circulation inevitably involves transferring personal data to third-party entities. Therefore, the personal data circulation stage should pay special attention to the authorization of personal data subjects for data circulation, as well as conducting thorough investigations into the necessary qualifications and capabilities of third-party entities. In specific operations, special attention should be paid to obtaining users' re-consent during data circulation and clearly defining the responsibilities of third-party entities.

6 Conclusions

This paper has constructed legal risks covering the four links of data collection, storage, use, and external provision, and proposed risk prevention measures for customer data to provide tool support for the legal and compliant application of customer data. In the collection link, the company should update relevant notification and consent rules in a timely manner and strictly abide by the principle of minimum necessary. In the storage link, the company should properly store data in accordance with the privacy agreement and improve its own data storage management mechanism. In the use link, the company should strictly use data within the scope authorized by the privacy agreement and seek re-consent in a timely manner under new circumstances. In the link of data external provision, the company should pay attention to the division of responsibility. The research results of this paper will provide compliance guidance for enterprises in customer data commercialization operations such as data application scenario development and business model design. It provides management ideas and risk prevention strategies for the legal and full use of customer data and provides better compliance protection for the development of the digital economy.

References

1. Pamela,S.(2000)Privacy as Intellectual Property.Stanford Law Review, 52:1125-1169.https://people.ischool.berkeley.edu/~pam/papers/privasip_draft.pdf.
2. Gao, F.P.(2019)Data production theory: the fundamental theory of the right allocation of data resources. Jiaotong Law Review,4:5-19.DOI:10.19375/j.cnki.31-2075/d.2019.04.001.
3. Liu, Z.G.(2018)The "Post-Privacy" Transformation of EU Personal Data Protection. Journal of East China University of Political Science and Law,4:54-64. https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C44YLTlOAiTRKibYlV5Vjs7i0-kJR0HYBJ80QN9L51zrP55eNts1epXCSj4Lc9wsltanpEJTdK03NUPIrP6pt7cv&uniplatform=NZKPT.
4. European Commission,2018.Study on data sharing between companies in Europe, .https://publications.europa.eu/resource/cellar/2d6d436e-4832-11e8-be1d-01aa75ed71a1.0002.01/DOC_1.
5. Yi, L.(2022)Study on the balance model of personal data protection and commercial utilization in EU law. German Research,5:80-96+116.https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C44YLT-lOAiTRKibYlV5Vjs7ioT0BO4yQ4m_mOgeS2ml3UP7jCYnwHET0rRJVw8HbPw4MGJdncx16DocSLRgsO4lQ&uniplatform=NZKPT.
6. Cheng. X.(2018) On Personal Data Rights in the Era of Big Data. Chinese Social Sciences, 3:102-122+207-208. https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C44YLT-lOAiTRKibYlV5Vjs7i0-kJR0HYBJ80QN9L51zrP3f6vEMjmrQVjL-OZbavGY9rLC1YBQPIZL0syWAweGtT&uniplatform=NZKPT.
7. Zheng, J.N.(2021)Exploration of the legal nature of data information property. Dongfang Law Review, 5: 43-56. DOI:10.19404/j.cnki.dffx.20210906.013.

8. Hu, L.(2021)Two types of property rights in the digital economy: from factors to architecture. Chinese and Foreign Law,6:1581-1598.https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C44YLTlOAiTRKibYlV5Vjs7iy_Rpms2pqwbFRRUtoUIm-HZOIKBXpQs0BRYxQrKqI5gznbQBt51meyu-MRbR0gE45&uniplatform=NZKPT.
9. Peng, C.X.(2021)On the dual legal nature of personal information. Tsinghua Law Journal, 6:78-97. https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C44YLT-lOAiTRKibYlV5Vjs7iy_Rpms2pqwbFRRUtoUIm-HXn62n94yB_i_9CA0vGp4YvweVn8tZh8fiIWIdy2g6yP&uniplatform=NZKPT.
10. Shi, Q. W., Cui, W. Q. (2018). The EU experience of protecting sensitive customer information. China Finance, 24, 92-93. https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C44YLTlOAiTRKibYlV5Vjs7iLik5jEcCI09uHa3oBxtWoIIRWVwgjljl4Ixx-PEIGsuTyuCIt6sQzC2oarwivV9vF&uniplatform=NZKPT.
11. Li, Z. Y., Li, X. (2017). The conflict and balance between financial group's customer data sharing and personal information protection in the era of big data. In: New Era Big Data Rule of Law Summit, pp.204-227. https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C467SBiOvrai6TdxYiSzCnOEARoQSLbIZ3uXK9jgHvAFzS5n5UDi-Cvb_4W4E4VZrq3GyVq3-sXs-5NuArNGe2Tt8wv2nsKsBilE%3d&uniplatform=NZKPT.