INDUSTRY NEWS

China's Personal Financial Information Protection

Author: Andrea Tang, FIP, CIPP/E, CIPM, ISO27001LA
Date Published: 22 February 2021

On 8 December 2020, the chairman of the China Banking and Insurance Regulatory Commission (CBIRC) laid out areas that the authorities will be looking at closely in the fintech industry. The growth of fintech in China is rapid, partially because of the massive use of epayments by 2 dominant players in the mobile payments space: Alipay and WeChat Pay. However, this growth in fintech means that there are likely challenges that need to be considered. What is the regulatory landscape in China with regard to personal financial information? How do these regulations impact global financial institutions? What are the

similarities and differences between the EU General Data Protection Regulation (GDPR) and Chinese laws? What are the next steps for both Chinese and global financial institutions?

Fintech Challenges

The first challenge is a massive amount of personal information processing. Many technology enterprises excessively collect, use and even sell information, possibly without obtaining consent from customers and, therefore, infringing on enterprise and individual privacy. Another challenge is third-party risk management. Many third-party payment platforms play roles in financial services, which makes it more difficult to regulate the investment functions on suppliers. There is also a lack of regulatory requirements. Because there are no laws governing personal financial information protection in the financial industry, let alone fintech, the missing gaps bring challenges to promoting regulatory operations.

The violation of any regulations or privacy laws not only damages an enterprise's reputation, but also imposes a large amount of economic penalties. On 28 July 2020, The Shanghai Supervision Bureau of CBIRC imposed ¥1 million (US$150 thousand) in fines, respectively, to 2 Chinese banks that failed to properly protect consumers personal information.

Laws, Regulations, Guidelines and Standards in China

Although China has not published any laws on personal financial information protection yet, 2 related draft laws are under review. However, there has been guidance published on personal information and mobile applications, and a series of financial industrial standards assisting financial institutions with compliance.

Draft Laws: Personal Information Protection and Data Security

In October 2020, China submitted a highly anticipated draft of the People's Republic of China on Personal Information Protection (PIPL)[1] law to the Standing Committee of the 13th National People's Congress for first review. It contains 8 chapters and 70 articles in line with Chinese Civil Code[2], which serves as the foundation for China's law framework. Chapter 6 of the code, "Privacy Right and Personal Information Protection" indicates the expanding scope of personal information and obligations on personal information processors. The draft PIPL also extends the application to processors outside of China. In addition, it regulates specific rules on sensitive personal information, requiring separate consent from individuals. It also replaces consent-based processing with multiple legal bases, including contract, obligations and public interest. The protection of individual rights when conducting automated decision-making has also been added as a consideration. Another draft law on Data Security (DSL)[3] was submitted on 2 July 2020. DSL is a multilevel classified protection regime depending on the importance of

data, which is defined by ministries and local governments. Important data processors are required to periodically conduct risk assessments and appoint data security officers and management departments to be responsible for data protection.

Guidance: Personal Information Protection and Applications

Although the 2 draft laws are still under review, the State Administration of Market Regulation and the Standardisation Administration of China has published a series of guidelines. The Information Security Technology-Personal Information Security Specification Revisions (GB/T 35273-2020)[4] went into effect on 1 October 2020, providing specific requirements to enhance protection of personal information. The Guidance for Personal Information Security Impact Assessment (GB/T 39335-2020)[5] will be effective on 1 June 2021, providing support to Art. 54 in PIPL. As for regulations on applications, the National Information Security Standardization Technical Committee (TC260)[6] and the Cyberspace Administration of China (CAC) have issued a series of guidelines and standards on data processing activities by mobile applications operators, covering self-assessment, use of software development kits and minimum scope of personal information necessary for function.

Financial Industrial Standards

Many financial industrial guidelines have also been published by the People's Bank of China (PBOC), including the following:

- **Personal Financial Information Protection Technical Specification (JR/T 0171-2020)**—Issued on 13 February 2020, it dictates that personal financial information should be classification into 3 levels and 7 categories.
    - **Levels by sensitivity**—User identification information (C3), information that can identify personal identity and financial status (C2) and internal information assets (C1)
    - **Categorization**—Account information, identification information, financial transaction information, personal identity information, property information, loan information and other information reflecting certain situations of specific financial information subject[7]
- **Financial Data Security—Guidelines for Data Security Classification (JR/T 0197-2020)**—Issued on 23 September 2020, it requires that data security should be divided into 4 levels from high to low with regard to the impact on national security, public interest, privacy and enterprise legal rights and the degree of impact caused by damage to the data security of financial institutions.[8]

- **Measures on the PBOC on the Protection of Financial Consumers' Rights and Interests (PBOC [2020] No. 5)**[9] —New measures were issued on 1 September 2020 and enacted on 1 November 2020. Compared with the regulation issued in 2017,[10] there are 5 significant changes:

1. An increased legal effect with upgrades to departmental regulations. Violation of the new regulations may be a violation of criminal law. (New measures Art.64)

2. A dynamic application scope in which institutions and enterprises each have their own standards, which determine the dynamic scope of application (New measures Art.52)

3. Concern about the 8 rights of financial consumers, which regulate detailed requirements on the right to property security, the right to be respected and the right to informed and fair trade that strengthen the right of information security and weaken the right of personal information control (New measures Art.14-21)

4. Standardization of direct marketing focused on the right to be informed (New measures Art.30)

5. Increased penalties for violating laws and regulations, with penalties of up to ¥500 thousand (US$74 thousand) (New measures Art.60 and the China Consumer Rights and Interests Protection Law[11])

Global Impacts on Financial Institutions

In addition to the economic penalties for violating the rights of Chinese citizens, national security and public interest, the CAC will place violating organizations on a blacklist. Applicable scenarios for overseas financial institutions in relation to collection personal financial information in China include:

- Localized processing of personal data when the processing takes place in China
- Processing of personal data by individuals or organizations outside of China that damages the interests of those within China's borders:
    - The provision of products or services to data subjects in China
    - The monitoring of their behavior as far as their behavior takes place within China
    - Other circumstances as provided by Chinese laws and regulations

Mapping the Chinese Laws to GDPR

China's draft PIPL is one of 12 GDPR-related privacy laws throughout the world, including the Australia's Privacy Act, Brazil's Lei Geral de Proteção de Dados (LGPD), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), Chile's Data Privacy Law, India's Personal Data Protection Bill (PDPB), Japan's Act on Protection of Personal Information, New Zealand's 2020 Privacy Act, South Africa's Protection of Personal Information Act (POPIA) and the Privacy Act, South Korea's Personal Information Protection Act, Thailand Personal Data Protection Act (PDPA) and the US State of California Consumer Privacy Act (CCPA).[12] **Figure 1** illustrates the comparisons between the PIPL and the GDPR.

Figure 1—Figure 1—Similarities and Differences Between GDPR and PIPL

Similarities	Differences
• Broad applicability beyond physical jurisdictions (PIPL Art.3). • Potential large fines for violations—fines up to ¥50 million (US$7.44 million) or up to 5% of the preceding year's turnover in China (PIPL Art.62). • ights of individuals in personal information processing activities, including rights to know, restrict or refuse, access and copy, correct, delete and explain the rules on personal information processing (PIPL Art.44-49).	• The draft PIPL does not differentiate between a data controller and data processor (PIPL Art.9). • Personal data processors and critical information infrastructure operators (CIIO) processing personal information over certain amounts within the territory of China are subject to the data localization requirement, and any cross-border data transfer is subject to security assessment to be conducted by the Chinese regulators (PIPL Art.40). • Sensitive information including financial account information requires separate consent in China (PIPL Art.30). • Parental consent is required for processing personal data of minors under the age of 14 (PIPL Art.15). • Lawfulness of processing does not include legitimate interest in China (PIPL

Similarities	Differences
	Art.13).

Compliance for Global Financial Institutions

The upcoming laws and regulations in China may create obstacles for global financial institutions doing business in China. Global financial institutions can do the following to proactively be in compliance with the Chinese regulatory landscape:

- Establish a specific department or designate personnel to supervise information processing in China
- Publish privacy notices for customers and employees in Chinese institutions
- Manage Chinese personal financial information
- Establish and maintain records of processing activities with regard to Chinese personal financial information
- Mark data dictionary, draw up personal data mapping and data transfer map
- Update cross-border data transfer contracts, standard contractual clauses

Next Steps for Chinese Financial Institutions

One of the pain points of personal financial information protection is data governance. Financial institutions should balance data sharing and data protection. For example, clarify under what circumstances consumers' big data can be used for commercial purpose needs and determine data retention periods and the degree of data sharing. These step-by-step guidelines on personal financial information protection may be useful:

1. Classify personal financial information:
    - Establish a complete classification of personal financial information.
    - Determine the technical safety requirements for the entire data life cycle.

- Update data mapping and the data dictionary by identifying personal information transfer scenarios, identifying third parties involved in the process of personal financial information transfer or exchange and proposing specific technical requirements.

2. Implement administration procedures:

   - Update privacy statements and notices from official websites and mobile banking applications and the internal privacy policy and agreement or contract signed by customers and employees.

   - Implement a data breach incident plan and procedures and data subject rights response procedures (i.e., implement the process of supplementary deletion of personal information and cancellation of user accounts and personal impact assessment procedures).

   - Establish a regular audit plan to evaluate the effectiveness of personal information protection policies, relevant procedures and security measures.

3. Appoint a person to oversee personal information protection and establish communication mechanisms:

   - Clarify the roles and responsibilities such as establishing the organizational structure of personal information protection and clarifying the roles and responsibilities of related departments.

   - Establish and improve internal and external communication.

   - Conduct privacy awareness training.

4. Transform IT systems involved with personal information protection:

   - Implement relevant IT systems and mobile apps transformation including collecting explicit consents, specifying the collection of sensitive personal information and data retention periods and providing customers with the right to object to direct marketing.

   - Categorize related IT systems and implement IT transformation for local maintenance systems, and update service level agreements (SLAs) and statements of work (SOWs).

Conclusion

In the era of digital transformation, more financial institutions are largely employing new technologies such as automated decision-making and artificial intelligence (AI) to provide customers with better services. With these new technologies, large amounts of personal financial information, especially sensitive personal information, is being processed. Therefore, it is important to balance consumer rights and services as personal financial information has social, economic and governance values. Although China's draft laws addressing personal information protection and data security are still in review, Chinese regulators are keeping a close eye on the financial industry as it is highly regulated and high risk. Therefore, financial institutions around the world providing financial services to the Chinese market should proactively take appropriate administrative and technical measures to meet the changes in the Chinese privacy regulatory landscape.

Endnotes

[1] The Standing Committee of the National People's Congress (NPC), Personal Information Protection Law of the People's Republic of China (Draft), China, 21 October 2020
[2] The National People's Congress of the People's Republic of China, Civil Code of the People's Republic of China, China, 28 May 2020
[3] The National People's Congress of the People's Republic of China, Data Security Law (Draft), China, 2 July 2020
[4] The State Administration of Market Regulation and the Standardization Administration of China, Information Security Technology-Personal Information Security Specification Revisions (GB/T 35273-2020), China, 6 March 2020
[5] The State Administration of Market Regulation and the Standardization Administration of China, Information Security Technology- Guidance for Personal Information Security Impact Assessment (GB/T 39335-2020), China, 19 November 2020
[6] National Information Security Standardization Technical Committee (TC260), China
[7] The People's Bank of China, Technical Specification for Personal Financial Information Protection (JR/T 0171-2020), China, 13 February 2020
[8] The People's Bank of China, Financial Data Security—Guidelines for Data Security Classification (JR/T 0197-2020), 23 September 2020
[9] The People's Bank of China, Measures on the PBOC on the Protection of Financial Consumers' Rights and Interests (PBOC [2020] No. 5), China, 1 September 2020
[10] The People's Bank of China, "Notice of the People's Bank of China on Issuing the Implementation Measures for the Protection of the Rights and Interests of Financial Consumers of the People's Bank of China", China, 4 July 2017
[11] The Standing Committee of the National People's Congress (NPC), China's Consumer Rights and Interests Protection Law, China, 27 August 200
[12] Simmons, D.; "12 Countries With GDPR-Like Data Privacy Law", Comforte, 17 January 2019

Andrea Tang, CIPP/E, CIPM, ISO27001 LA

Works at Ernst & Young providing privacy services to financial institutions. She serves as the leader of the ISACA© China WeChat group. She is an invited speaker for the Hong Kong Baptist University School of Business, Master of Science FinTech and Data Analytics program. Tang has published privacy-focused articles in the ISACA Journal and contributed to guidebooks released by the ISACA China Technical Committee.

Previous Article

Next Article

QUICK LINKS

Resources

COBIT

ISACA Journal

Press Releases

Resources FAQs

Insights and Expertise

Audit Programs and Tools

Publications

White Papers

Engage Online Community

News & Trends >

@ ISACA

Industry News

ISACA Now Blog

ISACA Podcasts

ISACA TV

Frameworks Standards and Models >

IT Audit

IT Risk

Glossary

Call for Case Studies