The Impact of PIPL on Asset Management Business

By Sandra Lu | Xun Yang | Tracy Chen

The Personal Informational Protection Law ("**PIPL**") has come into effect on 1 November 2021. It has for the first time set out comprehensive rules on protection of personal information, regardless of whether the information is recorded in an electronic or paper form or whether the information is about clients or employees. PIPL imposes stricter personal information rules on those handling personal information and thus has significant impact on all kinds of businesses, including, in particular, the asset management business.

I. An Introduction to PIPL

PIPL was not drafted from scratch. Rather, it reflects the personal information practice since the effectiveness of the Cyber Security Law in 2017. It also addresses a number of issues in the personal information protection regime which have long been controversial. It is determined to be milestone legislation on personal information protections.

"Personal information protection" had not been a recognizable concept in the Chinese legal culture until the wide use of information technology. It has been attracting more and more attentions when personal information is becoming increasingly important assets of business and abuse of personal information may cause increasingly significant losses.

如果您需要本出版物的中文本,
请联系:

Publication@llinkslaw. com

For more Llinks publications, please contact:

Publication@llinkslaw.com

China started to legislate on personal information protection in 2009 when stealing and sales of personal information was criminalized. The Standing Committee of the National People's Congress promulgated a decision to protect personal information in electronic forms in 2012 and the Ministry of Industry and Information Technology enacted an administrative rule on protecting personal information of telecoms users and internet users. In 2014, the Consumer Interest Protection Law was amended to include a clause to protect personal information of consumers. The Cyber Security Law effective in 2017 contains high level provisions on personal information protections and significantly improved personal information protection awareness. The Civil Code effective in 2021 has a chapter specifically for personal information, which confirms individuals' rights in their personal information.

All these laws, regulations, and administrative rules are still valid and relevant to personal information protections at certain aspect. They apply to personal information handling activities despite of the effectiveness of PIPL. For example, to the extent that individual investors' information is collected and processed via mobile client, the information is considered information of internet users and the MIIT rule on protection personal information of telecoms users and internet users will apply.

Correspondingly, a number of government agencies will participate in enforcement of PIPL. With respect to an asset management business, in addition to the regulators (e.g. CSRC, CBIRC) which will have imposed relevant requirements on information protection based on industry characteristics, the Cyberspace Administration of China ("**CAC**") and its local counterparts will be a core authority enforcing PIPL. Additionally, the State Administration for Market Regulation and its local counterparts will enforce PIPL from the financial consumer interest protection aspect; the Ministry of Public Security and its local bureaus will enforce PIPL from the network security aspect; the Ministry of Industry and Information Technology will enforce PIPL where personal information is collected or process via internet portals, Apps, and otherwise via public networks.

It is worth mentioning that PIPL set out a potentially high amount of administrative penalty for those violating the obligations under PIPL. As a result, a breach of PIPL may result in administrative and civil liabilities, and in serious cases, even in criminal liability.

II. Relevancy to Asset Management Business

PIPL sets out comprehensive and strict rules on protection of personal information. Since an asset management business may involve the handling of a high volume of personal information, PIPL will affect the specific design of business scenarios in the future. In particular, an asset management institution must pay attention to the following aspects from which PIPL develops the personal information protection rules.

(1) PIPL provides for a series of legal grounds where personal information can be handled. In addition to "notification and consent" which has been long considered the necessary legal ground for handling personal information, PIPL, for the first time on the national law level, broadens the grounds for handling personal information, including, among others, the circumstances where it is necessary to

perform contractual obligations or to perform statutory obligations. In the asset management business, some of the information which asset management institution collects is merely for performing asset management services and some of the information is collected due to asset management institutions' statutory duties. Therefore, asset management institutions may consider leveling on these ground to reduce their burdens to implement "notification and consent."

(2) PIPL has provisions specifically for protection of sensitive personal information. For example, the handling of sensitive personal information must seek separate consents from the relevant individuals and be subject to the conditions of "particular purpose", "sufficient necessity", and "strict protection measure". An asset management institution, especially a retail asset management institution handles a large amount of sensitive personal information in terms of financial account, KYC, investor suitability, etc., and thus must pay attention to these requirements.

(3) Similar to GDPR, PIPL grants relevant individuals the right to control the personal information relating to them. These rights include the right to know what personal information has been collected or processed, the right to have a copy of the personal information being collected or process, the right to update or correct or delete the personal information, the right to withdraw consents to personal information handling, and the right to transfer personal information. Given that an asset management institution may retain personal information of a large number of clients, the duty to respond to these individual requests may significantly increase its administrative burden.

(4) PIPL shifts the burden of proof of "fault" on the defendant personal information handlers to facilitate the establishment of a personal information infringement claims. In other words, in case of personal information infringement, if the party which handles personal information fails to prove its innocence, it will be presumed to be faulty. This would require asset management institutions to well establish and implement their personal information policies. Otherwise, it would be difficult for them to prove their innocence.

III. Business Scenarios to be Affected by PIPL in Asset Management Industry

Asset Management Industry may need to improve the handling of the personal information in accordance with the requirements of PIPL in the following business scenarios:

1. Collection of Individual Separate Consents and Public Disclosure of Personal Information Handling Rules

"Informed consent" is not a new invention by PIPL, but PIPL sets out stricter and more comprehensive rules on how to obtain "informed consent".

Article 41 of the Cyber Security Law provides that, when collecting and using personal information, network operators must follow the principles of lawfulness, legitimacy and necessity, publicly disclose the rules for collection and use of personal information, explicitly state the purpose, methods and scope of collection and use of personal information. On January 23, 2019, four ministries -- the CAC, the Ministry of Industry and Information Technology, the Ministry of Public Security, and the State Administration for Market Regulation – launched a special campaign against illegally collecting and using personal information via Apps, in which "not publicly disclosing collection and use rules" was listed as a critical focus violation of laws and regulations that infringes the rights and interests of users. Afterwards, to implement the special campaign, the four ministries jointly issued Measures for Determining Illegal Behavior in Collecting and Using Personal Information via Apps on November 28, 2019, and made it clear that when an App runs for the first time, it must prompt the users to read the collection and use policy such as privacy policy via pop-up windows or other obvious means, and the privacy policy must not be difficult to access or read. Information Security Technology—Personal Information Security Specification issued in 2020 further provides a template personal information protection policy for market participants' reference. As for PIPL, it further clarifies the scope of situations where individual consent should be sought (namely, notification obligation) and the obligations to obtain separate consent for handling sensitive personal information, providing personal information to other personal information handlers, cross-boundary transfer of personal information, etc.

Therefore, most asset management institutions have already put personal information protection policies[1] on their electronic platforms such as websites, Apps, etc. in accordance with the aforesaid rules. Such policies have largely met the requirements of publicly disclosing the scope, purposes and methods of handling personal information. In addition to updating the personal information protection policies in accordance with PIPL, sufficient attention shall be paid to the following three aspects related to the particularity of asset management industry:

(1) How to obtain the individual's separate consent

In the asset management industry, especially in the retail asset management sector, the handling of personal information is not always limited to performing statutory duties or obligations. For the purpose of improving its service quality and client acquisition rate and making tailored recommendation on the products on an ongoing basis, etc., asset management institutions may process and analyze the position traits, transaction records, status of profit and loss, etc. of individual financial accounts, or even utilize big data technology to perform customer profiling on specific types of customers. Such practice can not only improve the quality of their future asset management services, but also provide decision-making basis for the future policy formulation of regulatory authorities. As mentioned above, the handling of such personal information is

[1] Currently, it is a common practice in the industry to name such policy as "privacy policy" by referring to the overseas practice. However, it is worth noting that Chapter Six of Book Four "Personality Rights" of the Civil Code treats privacy and personal information as different subjects in providing civil protection. Considering that the rules and policies formulated to implement personal information protection only involve personal information handling, but not the personal privacy protection under the Civil Code, we suggest that the title of such policies shall be changed from "privacy policy" to "personal information protection policy".

regarded as handling of sensitive personal information and is subject to relevant individual's separate consent. The contents of such notification must be different from those for general personal information. Individuals have the right to reject such handling of personal information by asset management institutions or withdraw their consent. Asset management institutions shall not refuse to provide financial products or services on the ground that an individual does not provide consent to such handling of his/her personal information or withdraws the consent.

Regarding the approach to seek separate consent, by referring to the Information Security Technology—Guidelines for Personal Information Notices and Consent (Draft for Comments) issued by Standardization Administration on May 14, 2021, separate consent means informing the subject of personal information of the purposes, methods and scope of personal information handling, as well as the storage period, security methods and other rules separately **through the means such as enhanced or instant notifications** for personal information handling activities for certain particular business functions or certain purposes, and seeking explicit consents from the subject of personal information. **The separate consent process must not be tied to any irrelevant business function or handling purpose.**

Therefore, for the information handling activities which need separate consent of related individuals, how to integrate the module of separate consent, how to determine the scope of notification, and the impact on follow-up information handling after individuals refuse to provide or withdraw separate consent shall receive special attention in compliance with PIPL.

(2) How to obtain separate consent of clients sourced from distributors

For clients from direct sales, even if it is necessary to comprehensively consider the impact of factors such as customer experience, system transformation costs, and the implementation of subsequent data processing and analysis on the business, in general, asset management institutions can still add the modules for public display/notification of rules or obtaining individual consents to business scenarios. However, for clients sourced from distributors who do not have direct contact with asset management institutions, if the asset management institutions still consider including the such clients' financial account information into the big data statistical analysis, and the distributors are unable or unwilling to provide necessary assistance, such handling activities may not be conducted due to the lack of individual's separate consent.

It is true that due to the complexity of business models and the diversity and variability of personal information handling purposes, it is not in line with the principle of economic efficiency to include lengthy personal information protection policy in the legal documents such as asset management contracts. Or otherwise, if personal information policies need to be updated, asset management contracts shall be modified as well, which may involve complicated procedures. Therefore, we do not recommend to include all the contents of personal information protection policies or the matters requiring separate consent in asset management contracts and then obtain individual's separate consent through modes such as setting separate check boxes in the same contracts. However, as clients sourced from distributors do not have other direct connection with the asset management institutions, the asset management institutions may need to consider including certain special matters in the asset management contracts, product key facts statements, and other legal documents that need to be signed by such clients, to fully utilize all business steps to prevent legal and regulatory risks.

(3) Personal information in the institutional investors' information shall not be ignored

The information protected by PIPL is the personal information of natural persons. As most of the information of the institutional clients handled by asset management institutions is not personal information and is generally subject to data security related laws and regulations. However, it is noteworthy that when establishing business relationships with institutional investors, for the purpose of entering into a contract or fulfilling the KYC obligations, asset management institutions need to collect the information of legal representative, beneficiary owner, and ATTN, which is personal information. Thus, in business scenarios related to institutional investors, asset management institutions shall still pay attention to the notification of handling rules, or even individual consent under special circumstances, for personal information handling.

2. Management of Third Parties

PIPL provides several scenarios for personal information transfer, including providing personal information to third parties, entrusting the handling of personal information to others, etc. There are different personal information protection requirements for different scenarios. The business process of asset management business is complex, and the investors' information will be handled by several parties under different scenarios. An issue in any part of the business process may result in corresponding liabilities on asset management institutions, and thus one of the difficulties for asset management business to implement PIPL is how to prevent third party risks. From the perspective of the protection of investors' personal information, third-party institutions can be divided into 2 categories, one is the institutions involving personal information handling, such as distributors, fund administrators and other cooperating institutions, and the other is other ordinary institutions that may only have exposure to personal information rather than handling personal information. The management of the latter mainly focus on the lawfulness of personal information transmission. For example, according to the Measures for the Administration of Information Technology of Securities Funds Operating Institutions which was issued by CSRC, information technology service organizations shall not intercept, store, forward or use customer information. Thus, in cooperating with information technology service organizations, asset management institutions must ensure that there is no interaction of customer information with such institutions.

With respect to the cooperation with the institutions involving personal information handling, asset management institutions must pay special attention to PIPL and other relevant laws, regulations and national/industry standards on personal information transmission, joint handling of personal information, and entrusted handling of personal information. The pre-procedures, the division of responsibilities and liabilities between the information transferor and the information recipient, and the relationship with the personal information subjects (whether consent is required) differ under different scenarios of personal information handling. Thus, to manage such cooperating institutions, asset management institutions must determine the legal relationship with them when handling personal information in the first place, i.e. determining whether it is entrusted handling, providing personal information to another handler or joint handling, and whether it involves multiple types of the above legal relationship. For example, for the relationship between distributor and asset management institution, if a distributor provides KYC information related to anti-money laundering to the asset management institution, this is provision of personal information to another personal information handler. If such handling of personal information is necessary for the purpose of performing legal duties or obligations, no individual's separate consent is required. However, if the information provided exceeds the statutory scope, such as sharing of personal portrait information, individual's separate consent is required. Besides, if asset management institutions entrust distributors to collect additional identity information (such as checking whether a client is a US person) according to their business requirements, the relationship between distributor and asset management institution will also involve entrusted handling of personal information.

After determining the legal relationship involved for each handling purpose, asset management institutions shall take measures such as setting up different impact assessment procedures, clarifying the division of responsibilities and liabilities between the parties, and implementing different anti-leakage information technology measures in accordance with laws and regulations to effectively perform their obligations on personal information protection.

3. Management of Cross-border Transfer of Personal Information

In addition to conducting asset management by investing in domestic investments, asset management institutions may invest in overseas investments via mechanism such as QDII, QDLP, QDIE, and invest in overseas assets after obtaining relevant qualifications. For such overseas investment, overseas institutions may request PRC asset management institutions to provide personal information of the end investors in order to fulfill local anti-money laundering, sanctions list monitoring and other obligations.

It is noteworthy that, according to Article 38 of PIPL, if personal information handler needs to transfer personal information outside of the PRC due to genuine business needs, one of the following conditions must be met: (1) passing a security assessment conducted by CAC in accordance with Article 40 of PIPL (which applies when the institution is determined as a critical information infrastructure operator or when the personal information the institution has handled reaches the threshold prescribed by CAC); (2) Performing personal information protection certification via professional institutions in accordance with the requirements of CAC; (3) Entering into a contract with overseas recipient in accordance with the standard contract formulated by the CAC, and stipulating the rights and obligations of both parties; (4) Other conditions prescribed by laws, administrative regulations or requirements of CAC.

On October 29, 2021, CAC released the Measures for Security Assessment of Cross-boundary Data Transfer (Draft for Comments). In accordance with this consultation paper, in the event of “providing personal information abroad by personal information handlers who handle the personal information of more than **one million persons** ” and “providing **personal information of more than one hundred thousand persons** or **sensitive personal information of more than ten thousand persons** abroad **in aggregate**”, relevant personal information handlers shall apply to CAC via a local counterpart of CAC for security assessment of cross-border data transfer . Besides, professional institution certification, standard contracts and other supporting rules referred in PIPL have yet to be formally released.

In addition, the cross-border transfer of personal information is subject to further requirements such as personal information impact assessment for cross-border transfer of personal information, special “notification and consent” procedure towards personal information subjects, controls on the overseas recipient, and restricting the further provision of personal information to foreign judicial or law enforcement authorities.

IV. Compliance Advices for Asset Management Institutions to Implement PIPL

As PIPL has come into effect on November 1, 2021, in view of the particularity of the asset management business, we suggest to:

1. Establish and improve internal mechanisms related to personal information protection in accordance with laws

According to the requirements under both the PRC Data Security Law and PIPL, asset management institutions shall establish corresponding personal information governance mechanisms, including but not limited to:

(a) Establishing a whole-process data security management system that covers personal information;

(b) Developing work procedures and management systems relating to the collection, use and other relevant activities according to the handling purpose and methods of personal information, types of personal information, impact on personal interests, potential security risks, etc.;

(c) Implementing classified management of personal information on the basis of grading and classification of data;

(d) Managing the operational authority of personal information handling in accordance with the “minimum and need-to-know” basis

(e) Establishing personal information impact assessment mechanism to assess personal information handling activities that have major impact on personal rights and interests, like (i) handling of sensitive personal information; (ii) automated decision-making based on personal information; (iii) entrusted handling of personal information, providing personal information to other personal information handler and publicly disclosing personal information; (iv) cross-border personal information transfer;

(f) Establishing a convenient application acceptance and handling mechanism for individuals to exercise their rights;

(g) Sorting out the needs of cross-border personal information provision and establishing management system for cross-border transfer of personal information;

(h) Improving the management system of third parties; and

(i) Incorporating personal information handling activities into the scope of the company's contingency plan and compliance audit.

2. Improve the personal information protection policy and add separate consent modules

The duly disclosure of personal information protection policy and the record of obtaining personal consent are important evidence for the asset management institutions to deal with the disputes of infringement of personal information rights and interests in the future and to "prove that they are not at fault". It is also one of the aspects the competent authority would focus when inspecting whether the institutions effectively implement personal information protection. Asset management institutions must formulate personal information protection policies for online and on-site businesses that are in line with industry practices according to industrial characteristics, actual business conditions, and information interaction patterns with clients, and optimize the design of modules for individual separate consents.

3. Strengthening the management of third parties

In order to effectively prevent third party risks arising from personal information handling, and to ensure that the institutions themselves will not be involved in personal information handling violations by third parties, asset management institutions shall enhance due diligence on business counterparties, the ongoing and post supervisions and evaluation of third parties, and the division of responsibilities and liabilities of each party in the personal information handling in accordance with relevant requirements. Asset management institutions shall implement security measures according to actual legal relationships involved in specific cooperation model and the personal information handling activities, and cause the counterparty to sign relevant agreements on personal information handling as soon as possible to clearly stipulate the rights, obligations and legal liabilities.

If you would like to know more information about the subjects covered in this publication, please contact:

Sandra Lu
+86 21 3135 8776
Sandra.lu@llinkslaw.com

Xun Yang
+86 21 3135 8799
xun.yang@llinkslaw.com

Tracy Chen
+86 21 3135 8680
tracy.chen@llinkslaw.com

SHANGHAI

19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING

4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

SHENZHEN

18F, China Resources Tower
2666 Keyuan South Road, Nanshan District
Shenzhen 518063 P.R.China
T: +86 755 3391 7666
F: +86 755 3391 7668

HONG KONG

Room 3201, 32/F, Alexandra House
18 Chater Road
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON

1/F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.

© Llinks Law Offices 2021