International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 10 Issue 4, Jul-Aug 2026 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Legality Review of Securities Industry User Data Collection and Use: Based on the Personal Information Protection Law

Zhang Man Chi, Yu Sha Xin, Gong Xiao Chai, Li Jun Huan

Beijing Wuzi University, Beijing, China

ABSTRACT

Under the digital transformation of capital markets, securities firms' mobile applications have become the primary channel for investors to access online services, revealing problems such as excessive data collection, mandatory permission requests, and non-compliant data sharing. The Personal Information Protection Law establishes the general baseline for personal information processing, but the securities business involves special requirements such as suitability management and real-name account opening. The principled provisions of the higher-level law are difficult to implement directly, and the industry lacks standardized compliance operational guidance. This paper employs normative legal analysis, compliance assessment, and empirical research methods to conduct risk assessments on core business scenarios including account opening verification, suitability assessment, and data sharing. Drawing on regulatory penalty cases and field tests of securities firm applications, it identifies compliance shortcomings and develops a review checklist, proposing improvement measures from three levels: legislation, regulation, and institutional internal control.

KEYWORDS: *Personal Information Protection Law; Securities APPs; Investor Personal Information; Compliance Review; Investor Suitability.*

How to cite this paper: Zhang Man Chi | Yu Sha Xin | Gong Xiao Chai | Li Jun Huan "Legality Review of Securities Industry User Data Collection and Use: Based on the Personal Information Protection Law" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-10 | Issue-4, August 2026, pp.1131-1136, URL: www.ijtsrd.com/papers/ijtsrd141963.pdf

IJTSRD141963

I. INTRODUCTION

1. Statement of the Problem

FinTech has driven the digitalization of securities business, making online account opening and trading the norm, and the volume of investor information collected continues to expand. According to data from Analysys Qianfan, the monthly active users of securities APPs exceeded 168 million in 2025, representing a year-on-year increase of over 10%, reaching 175 million in December [1]. Securities firms extensively collect sensitive information such as user identity data, asset status, and transaction records. At the same time, the Cyberspace Administration of China (hereinafter "CAC"), the Ministry of Industry and Information Technology (hereinafter "MIIT"), and the China Securities Regulatory Commission (hereinafter "CSRC") have continuously rectified data compliance issues in securities mobile internet applications (hereinafter "APPs"). In July 2026, the MIIT notified 32 APPs and software development kits (hereinafter "SDKs") with infringing user rights, revealing frequent problems such as excessive data collection, mandatory permission requests, and illegal data sharing [2], highlighting the general weaknesses in securities firms' data governance.

Although the Personal Information Protection Law has established a top-level framework, and supporting rules such as the CAC's Administrative Measures for Personal Information Protection Compliance Audits and the Securities Association of China's (hereinafter "SAC") Technical Specification for the Protection of Investor Personal Information by Securities Companies have been continuously improved, there remains considerable room for improvement in the application of these rules to the securities industry. The core limitations lie in insufficient case comparisons, a lack of implementable tools, and limited survey samples and data coverage. To address these deficiencies, Chapter II systematically reviews the legal framework applicable to the collection and use of user data in the securities industry, providing a normative benchmark for subsequent empirical analysis.

II. Legal and Regulatory Basis for Compliance in Securities Industry User Data Collection and Use

The compliance normative system for securities industry data presents a three-tier structure: "general law as foundation, sector-specific law as pillar, and industry standards as beam." It consists of the core principles of the Personal Information Protection Law of the People's Republic of China (hereinafter the "PIPL"), the special rules of securities regulation, and the interplay between the two.

1. General Basic Norms under the PIPL

The PIPL establishes the baseline for personal information processing across all industries. The core principles are "lawfulness, legitimacy, necessity, and good faith," with "necessity" further developing into the "minimum necessity" criterion, requiring that information collection be limited to the minimum scope necessary to achieve the purpose of processing. In the securities context, securities firms may not bundle the collection of user data unrelated to services such as market quotation inquiries and trade execution beyond the specific purposes of those services.

"Informed consent" is the core safeguard for users' autonomy over their information [3]. Under Article 17 of the PIPL, before collecting information, the processor must inform the data subject in a prominent manner of the purpose, method, type, and retention period of processing, and obtain explicit consent. In practice, however, lengthy and obscure privacy policies and default checkboxes have nullified this rule. Where the provision of information to third parties or the processing of sensitive information is involved, the law also requires "separate consent."

Article 16 of the PIPL prohibits "forced consent" and "bundled authorization." For sensitive personal information, Articles 28 to 30 establish stricter authorization rules. Scholars have proposed shifting from a "subjective paradigm" to an "objective paradigm," whereby the reviewer determines the purpose of processing based on objective elements rather than the processor's unilateral statements [4]. In the data usage phase, users enjoy rights of access, copying, correction, deletion, and withdrawal of consent, and the processor must provide convenient withdrawal methods. The lack of withdrawal channels and the difficulty of account cancellation are prominent shortcomings in current securities industry data compliance.

2. Special Personal Information Protection Regulatory Rules for the Securities Industry

The Securities Law of the People's Republic of China (hereinafter the "Securities Law") expressly provides that securities firms have a duty of confidentiality over investor information and may not disclose it to any third party without statutory grounds or statutory procedures. When providing data externally, securities firms must comply with both the separate consent requirement under the PIPL and the confidentiality obligation under the Securities Law.

The Administrative Measures for Suitability of Securities and Futures Investors require operating institutions to understand investors' identity, property status, and investment experience to complete risk assessment. Information collected for this purpose is grounded in "necessity for performing statutory obligations," but must be strictly tied to the assessment purpose. The Administrative Measures for Cyber and Information Security in the Securities and Futures Industry explicitly prohibit the mandatory collection of biometric information and require the provision of alternative verification methods. The SAC's Technical Specification for the Protection of Investor Personal Information by Securities Companies is the industry's first systematic technical standard. The Administrative Measures for Personal Information Protection Compliance Audits require entities processing personal information of more than 10 million individuals to conduct a compliance audit at least once every two years, covering most large and medium-sized securities firms.

3. The Dual Compliance Constraint Logic in the Securities Industry

The above norms create a "dual compliance" constraint for the securities industry. The first layer comes from the general baseline of the PIPL, and the second from the special requirements of financial regulation. The two layers are parallel in legal effect and superimposed in application.

This draws a clear boundary between "statutorily necessary information" and "commercially unnecessary information." The former, such as identity, property, and transaction records collected for account opening verification, transaction record-keeping, and risk assessment, may be processed based on statutory obligations; the latter, such as behavioral data collected for precision marketing, must return to the informed consent framework. Securities firms may not convert the mandatory nature of performing statutory obligations into a convenience for obtaining commercial data authorizations. Chapter III systematically analyzes the current state of compliance in securities industry data collection and use, based on the regulatory notice data of the National Cybersecurity Notification Center since 2025.

III. Empirical Analysis of the Current Compliance Status of Securities Industry User Data Collection and Use

This chapter collects violation cases involving 14 securities firms and 16 APPs. Drawing on the notifications issued by the National Cybersecurity Notification Center from May 2025 to March 2026 and the notices of local communications administrations (hereinafter "local CAs") as core data sources, it categorizes and analyzes the violations involved. Overall, the compliance situation in the securities industry is not optimistic.

1. Overall Characteristics and Trends of Industry Violations

In 2025, the notifications of the National Cybersecurity Notification Center and local CAs involved a cumulative total of 14 securities firms and 16 APPs, showing an upward trend compared with 2024. The violations concentrated on three types: failure to list privacy policies item by item, failure to provide withdrawal channels for consent, and failure to adopt encryption and de-identification measures. Industry violations exhibited characteristics of intensive notifications, broad coverage, and prominent problems among small and medium-sized securities firms.

Throughout 2025, the National Cybersecurity Notification Center released multiple lists of illegal and non-compliant mobile applications, with financial institutions appearing in every list; as of July, it had cumulatively issued eight lists. The notified institutions covered a wide range from leading to small and medium-sized securities firms, with smaller institutions appearing significantly more frequently. The violations centered on three types: failure to list privacy policies item by item; failure to provide withdrawal channels for consent (35 apps involved in July 2025, the highest frequency in that period); and failure to adopt encryption and de-identification measures. These violations correspond to core compliance principles such as "informed consent," "minimum necessity," and "user rights protection" under the PIPL. The "purpose limitation principle" lacks quantitative boundaries in specific industry scenarios, which is an important reason why compliance standards are difficult to unify [5].

A summary of the notifications in each period: In June 2025, 64 APPs were notified, involving Cheng Tong Securities, Industrial Securities, Shen Gang Securities, and Minmetals Securities, all of which failed to inform the recipients of information and obtain separate consent. In July, 68 APPs were notified, involving Yin Tai Securities and Caida Securities; Yin Tai Securities was also involved in default consent and third-party sharing violations. In September, 69 APPs were notified, and Datong Securities was named for failing to list privacy policies item by item and for third-party sharing without consent and anonymization. In February 2026, 72 APPs were notified, involving Da Zhi Hui, Zhongshan Securities, etc., with high-frequency violations of "failure to prominently inform the data processing rules" (17 apps) and "failure to list privacy policies item by item" (34 apps). In March–April, 71 APPs were notified, and Huabao Securities' Huabao Smart Investment was named for providing personal information to third parties without notification, separate consent, or anonymization. From November to December 2025, the Shanghai Communications Administration inspected and found 71 APPs infringing user rights, involving Bank of China Securities (failure to specify rules, account cancellation difficulties), Shenwan Hongyuan Securities (account cancellation difficulties), and Oriental Securities (failure to specify rules, excessive permission requests, account cancellation difficulties); 38 APPs were delisted for failing to rectify, with a rectification completion rate of only 46.48%.

2. Four Typical Business Scenarios Mapped to Compliance Risks

The above violations can be categorized by business type into four core business scenarios.

A. Account Opening and Identity Verification Scenario

This scenario involves the collection of basic information such as name and ID number, as well as biometric information such as facial recognition and fingerprints. The core risk lies in whether the securities firm prominently fulfills its disclosure obligation and obtains explicit consent. Securities firms are important personal information processors, but there are still many loopholes in the consent notification process [6]. A typical case is Yin Tai Securities' Yin Tai Zhang Yi Bao, which failed to pop up a notice to read the privacy policy on first launch and obtained consent by default, violating Article 14 of the PIPL [7]. Oriental Securities' Oriental Winner had issues of "forced, frequent, and excessive permission requests." Compliance points: an independent pop-up window should be used to prompt reading of the privacy policy, and users should actively check the box to confirm; biometric information must obtain separate consent and alternative verification methods must be provided.

B. Data Entrustment Processing and Third-Party Sharing Scenario

Securities APPs generally embed third-party SDKs, generating a large amount of personal information provision to third parties. This scenario is the most frequent violation type among the notifications, with a total of eight firms named. The high-frequency violations are failure to inform the recipient of information and obtain separate consent, and failure to anonymize/de-identify. Compliance points: the recipient information should be notified and separate consent obtained in advance; information provided externally should be de-identified.

C. Investor Suitability Risk Assessment Scenario

This scenario is the most closely intertwined area between the PIPL and securities regulatory rules. The Administrative Measures for Suitability of Securities and Futures Investors require understanding investors' identity, property status, etc., to complete risk assessment [8]. High-frequency violations include risk assessment questionnaires that collect sensitive information beyond what is directly related to risk evaluation, and the use of assessment data for precision marketing. The Measures require "full use of already-known information and existing assessment results," but in practice some firms still collect beyond the scope.

D. Data Storage and User Rights Protection Scenario

The rules on active deletion after withdrawal of consent lack clear operational guidance in the financial context. High-frequency violations are failure to provide withdrawal channels and setting high thresholds for account cancellation. In July 2025, "failure to provide withdrawal channels" involved 35 apps, the highest frequency; in November, Shenwan Hongyuan, Bank of China Securities, and Oriental Securities all had "account cancellation difficulties"; in February 2026, Da Zhi Hui was cited for "failure to provide effective correction, deletion, and account cancellation functions." Compliance points: a convenient withdrawal channel should be provided in the settings interface (no more than 3 steps); a convenient account cancellation function should be provided.

To clearly present the analysis results, the cases are summarized in Table 4-1 below:

Account Opening & Identity Verification	Default consent, failure to specify rules, excessive permissions	PIPL Arts. 14, 17	Yin Tai Securities, Oriental Securities
Third-Party Data Sharing	Failure to inform recipient, failure to obtain separate consent, failure to anonymize	PIPL Art. 23	Cheng Tong/Industrial/Shen Gang/Minmetals Securities, Huabao Securities
User Rights Protection	Account cancellation difficulties, no withdrawal channel for consent	PIPL Arts. 15, 47	Shenwan Hongyuan, Bank of China Securities, Da Zhi Hui
Privacy Policy Compliance	Failure to list collection purposes/methods/scope item by item	PIPL Art. 17	Datong Securities, Zhongshan Securities

IV. Multiple Causes of the Compliance Dilemma in the Securities Industry

1. Gaps in Sector-Specific Supporting Rules under the PIPL

The PIPL tends toward framework-style principled provisions and does not set detailed rules for high-value financial information in the securities industry [9]. Investor information includes assets and transaction records, which are clearly different from ordinary internet information, and the existing law cannot adapt to business scenarios such as robo-advisory and customer risk control. Principles such as minimum necessity lack scenario-specific interpretation, and regulators have not issued positive and negative lists for data collection. The relevant SAC norms are only voluntary self-regulatory documents without mandatory enforcement effect. Cross-sectoral businesses such as intra-group data flows, AI investment advisory, and cross-border data transmission lack detailed supporting rules, and regulatory powers and responsibilities are unclear, leaving securities firms without a unified implementation basis for compliance construction.

2. Lack of Cross-Departmental Regulatory Coordination Leading to Divergent Enforcement Standards

Securities APP data compliance is subject to three parallel systems: the CAC's APP special rectification, the CSRC's industry compliance supervision, and local CAs' territorial enforcement. Different agencies govern under different laws, with different governance priorities and a lack of regular coordination mechanisms, forcing securities firms to repeatedly respond to different regulatory inspections. There is currently no unified testing standard for the securities industry, and different regulators cooperate with different third-party testing institutions, resulting in inconsistent findings on similar data violations, making it impossible for securities firms to confidently determine the direction of rectification.

3. Institutional Internal Control Deficiencies Constraining the Effectiveness of Self-Inspection Checklists

Securities firms in digital operations generally tend to collect and retain more customer data, and most institutions lack a management system covering the entire data lifecycle. Existing self-inspection checklists focus on system operation status and rarely verify legal compliance items, failing to correct the habit of excessive collection. Business, IT, and compliance departments work in silos, with compliance review lagging behind product development, and self-inspection checklists are mostly used only for ex post filing. Institutions lack regular audit mechanisms for third-party service providers and intelligent algorithms; merely checking boxes cannot identify real security risks.

V. Constructing Solutions to the Compliance Dilemma in the Securities Industry

1. Filling the Gap in Sector-Specific Supporting Rules under the PIPL

Regulators should issue detailed implementing rules for the securities sector, with the CSRC and the CAC jointly developing positive and negative lists for data collection covering all core business scenarios, and unifying the standards for determining the minimum necessity principle in the financial sector. The SAC‘s self-regulatory documents should be upgraded to mandatory industry standards, giving algorithm auditing and third-party management the force of enforcement. The CSRC should coordinate multiple departments to issue detailed rules for cross-sectoral businesses, unify regulatory standards, and periodically publish violation cases to guide industry compliance.

2. Building an Integrated Cross-Departmental Collaborative Regulatory System

A long-term multi-department joint governance mechanism should be established, with clear division of regulatory scope based on each institution’s functions, distinguishing three types of work: personal information protection, capital market security, and online application permission governance. Information sharing channels for enforcement should be opened, and case transfer procedures unified to reduce the compliance burden of duplicate inspections. A unified technical testing standard for securities industry APP data compliance should be issued to form standardized assessment criteria and stabilize securities firms‘ expectations for rectification.

3. Optimizing Institutional Internal Control Systems to Activate the Effectiveness of Compliance Self-Inspection Checklists

Regulators should issue a model compliance self-inspection checklist for the securities industry, explicitly requiring the addition of statutory verification items such as legality assessment of data collection, necessity verification of retention periods, compliance of dynamic permission management, and separate authorization verification for sensitive information. Securities firms should establish a compliance management system covering all stages of the data lifecycle [10], embed the checklist review into the front-end processes of product iteration and system development, and prohibit new businesses from going online without compliance review. Detailed self-inspection standards for external cooperation and intelligent algorithms should be developed [11], with separate entries for third-party SDK management, outsourcing audits, and AI investment advisory algorithm audits, and the establishment of access whitelists and annual audit systems.

VI. Conclusion and Future Prospects

Through systematic review of public regulatory penalty cases and preliminary field tests of three typical securities APPs, the main findings are as follows: in the four core scenarios of account opening verification, third-party sharing, suitability assessment, and user rights protection, securities firms’ user data compliance generally suffers from the contradiction of “formal completeness but substantive non-compliance”—the “check-the-box” consent in privacy policies is reduced to a legal disclaimer, and problems such as mandatory authorization, excessive collection, opaque third-party sharing, and lack of withdrawal and cancellation channels remain severe, especially among small and medium-sized firms. The dilemma stems from three levels: legislation, regulation, and enterprises: principles such as “minimum necessity” lack quantitative boundaries, ex post spot-check enforcement lacks sustained deterrence, and internal departmental coordination is broken. The “core business scenario compliance review checklist” developed based on current legal norms transforms abstract legal provisions into operable verification indicators, providing a practical tool for frontline compliance personnel of securities firms.

The empirical basis of this paper mainly relies on public regulatory penalty records and front-end functional tests of APPs, with a sample covering three types of securities firms. Future research may combine in-depth interviews and regulatory on-site

inspection reports to deepen understanding from an internal perspective, and expand the scope to frontier areas such as robo-advisory algorithm profiling, quantitative trading data integration, and virtual digital human interactive data collection. In these scenarios, the boundaries of data collection are more blurred and usage methods more concealed, and the effectiveness of the informed consent mechanism faces fundamental challenges, urgently requiring forward-looking theoretical and institutional responses.

References

[1] Shu Siqin, Hong Xining, Fang Li. Securities Industry Research: 2025 Net Profit Attributable to Parent +46%, ROE Increased to 7.31% [R]. Guojin Securities, 2026-04-02.

[2] Ministry of Industry and Information Technology, Information and Communications Administration. Notification of APPs (SDKs) Infringing on Users' Rights and Interests (2026, 4th Batch, Total 57th Batch) [Z]. 2026-07-02.

[3] Song Caifa. The Principles of Personal Information Protection, Reasonable Use, and Legal Protection [J]. Economic and Social Development, 2025, 23(5): 1-10.

[4] Wu Xianze. On the Objective Paradigm of the Purpose Requirement for Personal Information Processing [J]. Nanjing University Law Journal, 2024(6): 18-38.

[5] Wang Yuan. Rethinking the Purpose Limitation Principle and Its Interpretative Construction—Centering on Article 6(1) of the Personal Information Protection Law [J]. ECUPL Journal, 2024, 27(4): 44-53.

[6] Zhao Yin, Yang Jinqi. Securities Companies' Obligation of Personal Information Protection: Origins, Difficulties, and Breakthroughs [J]. Journal of Southwest University of Political Science and Law, 2022, 24(6): 67-81.

[7] Qian Yuwen. On the Regulatory Path of Consumer Financial Information Security [J]. Journal of China University of Political Science and Law, 2024(1): 5-18.

[8] Yin Huarong, Wu Yangyu. Legal Definition of Personal Financial Account Information [J]. Theory and Practice of Finance and Economics, 2024, 45(3): 154-160.

[9] Li Shengli, Cao Yanbing. Legal Issues of Worker Personal Information Protection in the Digital Age [J]. Journal of Tianzhong, 2026, 41(3): 33-40.

[10] Liu Quan. On the Person in Charge of Personal Information Protection—Centering on Article 52 of the Personal Information Protection Law [J]. Administrative Law Review, 2024(5): 116-131.

[11] Lin Zhonghua. Overseas Asset Auditing and Supervision of State-Owned Enterprises: Problems and Countermeasures [J]. Yangtze Tribune, 2016(2): 46-51.