Llinks Client Alert — August 2025
Want to Avoid APP Violations? Here's How!

APPs are increasingly becoming one of the most important marketing and customer acquisition channels for companies. However, the public accessibility of Apps also makes them a "compliance black hole" that is easily targeted. In addition to complaints from consumers and competitors, routine inspections and misconduct notifications from various regulatory authorities have become the norm. Currently, various regulators, including those from industry and information technology, cyberspace administration, public security, and market supervision, as well as their affiliated public institutions (such as the National Computer Virus Emergency Response Center), conduct irregular APP inspections and issue public notices for APPs that violate regulations. If a company fails to promptly rectify the issues mentioned in these notices, it may face penalties such as APP removal, disconnection of network access, fines, and even business suspension.

Therefore, APP compliance has become a top priority for companies' data compliance efforts. Rather than "locking the barn door after the horse has bolted" when an APP is flagged, a more effective approach is to be proactive in your daily compliance work, get ahead of APP compliance issues, and leave regulators with nothing to find fault with. In this client alert, we've combined legal requirements with our past experience helping companies respond to APP notices to summarize the key compliance points for avoiding APP violations.

1. Privacy Policy

A privacy policy has become the "face" of an APP and is a key focus during APP inspections and notifications. The main issue regulators focus on is "failure to clearly state personal information processing rules". To identify this, regulators simply need to review the APP's privacy policy. To avoid being flagged, companies should pay attention to the following:

1) Unless the APP collects no personal information at all, a privacy policy must be in place.
2) When the APP is launched for the first time, the privacy policy should be displayed prominently, such as through a pop-up window, to prompt users to read it.
3) After a user registers or logs in, they should still be able to view the privacy policy. It should be accessible within four clicks from the main interface of the APP.
4) For situations involving the collection/processing of sensitive personal information, cross-border data transfers, or data sharing, separate consent must be obtained. The display mechanism for this consent (such as a separate pop-up or checkbox) should be carefully chosen.
5) Regarding the content of the privacy policy itself, the following points should be noticed:

- List the purpose of collecting personal information and the types and fields of personal information collected in a one-to-one correspondence, avoiding mixing them together.
- Mark sensitive personal information types prominently (e.g., bolding, underlining, or italicizing the text).
- When sharing personal information with third parties, it's recommended to list the shared personal information and recipient information in a table format.
- For SDK information, clearly inform users of the name, function, type of personal information collected, and privacy policy link of any third-party SDKs embedded in the APP.
- If the APP collects/processes personal information of minors under the age of 14, there should be at least a dedicated section outlining the rules for processing their personal information.

2. Illegal Collection of Personal Information

The second major area of focus for regulators in APP notices is whether an APP's collection of personal information is legal, legitimate, and necessary. In this inspection, regulators will use a combination of APP usage and technical means to determine whether the APP's actual collection of personal information complies with legal requirements and the content of its privacy policy. To avoid being flagged, companies should be aware of the following:

1) Avoid collecting personal information before the user has agreed to the privacy policy.
2) Avoid collecting personal information beyond the scope authorized in the user's privacy policy, or processing personal information in a manner inconsistent with what was stated in the policy.
3) Avoid pre-checked consent boxes or bundled authorizations for privacy policies or pop-ups.
4) Even with a compliant privacy policy, you should still pay attention to the necessity of the personal information being collected/processed. Avoid collecting personal information that is irrelevant to the APP's functions or denying APP features because a user refuses to provide non-essential personal information. Furthermore, collecting personal information for broad purposes such as "improving service quality", "enhancing user experience", or "developing new products" has been considered a violation in past notices.

3. Forced Permission Requests

"Forced, frequent, and excessive APP permission requests" also appear frequently in APP notices. In this type of inspection, regulators primarily focus on the timing, frequency, and reasonableness of when an APP requests device permission. To avoid being flagged, companies should be aware of the following:

1) Before calling for a user's device permissions, consent should be obtained through a pop-up or other mechanism. Avoid enabling permissions by default.
2) Permissions should be requested in real time when the APP service or function requires them. Avoid asking for permissions prematurely.
3) Avoid repeatedly requesting a specific permission shortly after the user has declined it.
4) Do not request permissions that are irrelevant to the APP's services (e.g., a weather APP requesting contact permissions).

5) Except for permissions that are essential for the APP to run or provide its services, you should not deny related functions or services if a user declines to grant a specific permission.

4. Restrictions on User Rights to Personal Information

Regarding user rights to personal information, the main focus for regulators is "failure to handle user complaints properly" and "difficulties in account cancellation". In this inspection, regulators will act as a user and test the APP's functions that respond to user rights to determine whether the company responds to user requests in a legal and timely manner. Specifically:

1) For user requests and complaints:

- The APP's privacy policy should specify the channels and methods for users to exercise their rights as personal information subjects.
- It is recommended to set up a way for users to submit requests or complaints directly through the APP. If there are technical difficulties, then consider using phone or email as alternatives.
- If identity verification is required to respond to a user's request or complaint, the information requested for verification should be personal information that has already been collected during registration or use.
- For user requests and complaints received, it is recommended to provide feedback and a resolution within 15 working days.

2) For account cancellation:

- The APP's privacy policy should specify the method for users to cancel their accounts, and the APP should have an account cancellation feature.
- If identity verification is required for account cancellation, the information requested should be personal information that has already been collected during registration or use.
- Account cancellation should be completed within 15 working days, and no unreasonable conditions should be set to hinder the user from canceling their account.

5. Other Key Points

In addition to the main points mentioned above, the following APP violations have also been mentioned in some notices and should also be taken seriously by companies:

1) Minor Identity Verification: APPs related to gaming, live streaming, chatting, social media, e-commerce, and education should pay attention to whether a reasonable identity verification mechanism for minors has been implemented.
2) Auto-start and Associated-start: Avoid the APP starting on its own through system mechanisms without user operation, as well as the APP starting, waking, or jumping to other APPs without user operation

or authorization.

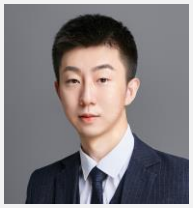
3) Random Pop-up Window Jumps/Inability to Close: Avoid clicking a pop-up window and jumping to an irrelevant page or APP. Also, avoid creating pop-up windows that cannot be closed or require a certain amount of time to be closed.
4) Automated Decision-Making: If an APP involves the use of automated decision-making to process personal information (e.g., using algorithms for personalized recommendations), it must provide an option that does not target the user's personal characteristics.
5) Whether Encryption and Other Technical Measures Are in Place: Regulators can detect whether an APP's data transmission is encrypted through methods like data packet capture and traffic analysis. Therefore, companies should take necessary encryption measures for APP data storage and transmission.

In the field of APP compliance, we can provide clients with the following services:

- Privacy by design and functionality during the APP development stage
- Drafting privacy policies and user agreements
- Comprehensive APP compliance assessments and improvements
- APP-related registration and filing
- APP security certifications
- APP security technical testing
- Assessment, rectification, and government communication after an APP has been flagged for violations

If you are in need of any of our legal services, please feel free to contact us:

David Pan
+86 21 3135 8701
david.pan@llinkslaw.com



Nigel Zhu
+86 21 3135 8683
nigel.zhu@llinkslaw.com

Susan Deng
+86 21 6043 3793
susan.deng@llinkslaw.com

Previous Articles

Llinks Client Alert (June 2025) - Is Purchased Data Risk-Free

Llinks Client Alert (June 2025) - Data breaches may be inevitable, but here's a roadmap to proper response

Llinks Client Alert (April 2025) - Embracing AI Are you ready compliance-wise?

Llinks Client Alert (December 2024) - What data compliance tasks are left to be done for 2025

Llinks Client Alert (November 2024) - Personal Data Protection Compliance Audit - Are you preapred?

Llinks Client Alert (October 2024) - Why is this new PRC data security regulation important to your 2025 data compliance work

SHANGHAI	BEIJING	SHENZHEN
19F, ONE LUJIAZUI 68 Yin Cheng Road Middle Shanghai 200120 P.R.China T: +86 21 3135 8666 F: +86 21 3135 8600	30F, Central Tower, China Overseas Plaza, 8 Guanghuadongli, Chaoyang District Beijing 100020 P.R.China T: +86 10 5081 3888 F: +86 10 5081 3866	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	LONDON
Room 3201, 32/F, Alexandra House 18 Chater Road Central, Hong Kong T: +852 2592 1978 F: +852 2868 0883	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