Draft Provision on the Collection and Use of Personal Information on Internet Applications Enhancements and Challenges

By Xun Yang | Yiran Li

The *Draft Provision on the Collection and Use of Personal Information on Internet Applications* (the "Draft Provision") was released by the Cyberspace Administration of China for public consultation in January, 2026, with a consultation period of one month. The Draft Provision was issued under the background of widely use of internet applications in all business sectors and an increasingly complicated business ecosystem comprised of, in addition to mobile and internet applications ("Apps"), software development kits (SDKs), distribution platforms, and intelligent terminals installed with Apps. It is also to consolidate maturing but fragmented regulatory instruments governing personal information protection in Apps, including those ministerial rules, normative notices, enforcement guidelines, and national and organizational standards targeting App compliance. The Draft Provision seeks to respond to these challenges by consolidating existing rules, elevating practical compliance experience into binding obligations, and extending regulatory attention from App operators to the entire App life cycle ecosystem.

I. Overview of the Draft Provision

The Draft Provision consolidates fragmented App personal information compliance requirements into a unified, life cycle–based regulatory framework that imposes explicit and enforceable obligations across App operators, SDK developers, distribution platforms, and intelligent terminal providers.

For more Llinks publications, please contact:

Publication@llinkslaw.com

(1) Key Features of the Draft Provision

A defining feature of the Draft Provision is that it is not designed as a wholly new regulatory regime, but rather as a consolidation and systematization of pre-existing requirements scattered across laws, ministerial regulations, and standards. For example, the obligation to establish and disclose "dual lists" of personal information collection and use, originally introduced in MIIT's "Information Service Enhancement Initiatives", is incorporated into the Draft Provision and further refined by requiring disclosure of permission names and invocation frequency. Similarly, SDK-related disclosure obligations that previously appeared in MIIT notices on "Improving Mobile Internet Service Capability" are restated and standardized, with more detailed elements such as SDK version, operator identity, and links to complete SDK privacy rules now expressly mandated.

Beyond consolidation, the Draft Provision translates regulatory practice into explicit compliance rules. Enforcement actions over recent years have revealed regulators' expectations regarding restrictions on excessive permission requests, and account cancellation procedures. These expectations, previously reflected mainly in enforcement notices or technical guidelines, are now codified. For instance, the previously closed look in grant of permissions in Apps in enforcement actions are codified into the Draft Provision as an explicit rule to require access to the album or contact list only when absolutely necessary and not earlier.

Another significant feature is the expansion of regulatory scope beyond App operators. The Draft Provision adopts a life cycle governance approach, imposing direct compliance obligations on SDK operators, App distribution platforms, and intelligent terminal manufacturers. This approach reflects regulators' recognition that personal information risks do not arise solely from App operators' conduct, but from the combined actions of multiple players included in the App ecosystem.

(2) Compliance Across the App Life Cycle Environment

Different from previous regulatory instruments which primarily focus on designs and operations of Apps, the Draft Provision sets out obligations for SDK operators, App distribution platform operators, and intelligent terminal manufacturers.

Under the Draft Provision, SDK operators are required to formulate and publicly disclose their own personal information collection and use rules on their official websites, a requirement that addresses the common industry practice of providing only fragmented or inaccessible disclosures. App operators, in turn, must contractually define the scope of personal information processing by embedded SDKs and adopt effective technical measures to audit SDK behavior, ensuring consistency between declared and actual data practices.

App distribution platforms assume a markedly enhanced role. In addition to strengthening pre-launch and update review, platforms must establish normative archives documenting Apps' personal

information practices, record compliance issues, and track regulatory notifications or administrative penalties imposed on Apps. They are further required to reflect the results of personal information protection certifications and App security certifications in their recommendation and display mechanisms, effectively introducing compliance-based differentiation in App visibility. Moreover, where an App has been subject to official notifications or penalties for unlawful personal information practices, distribution platforms must display a personal information security risk warning on the distribution and download page within six months after the public release of such official notifications or penalties.

Intelligent terminal manufacturers are similarly brought into the governance framework. Together with distribution platforms, they are required to accept complaints regarding pre-installed or distributed Apps and to urge App operators to rectify verified compliance issues. This reflects regulators' intent to leverage terminal-level control and complaint-handling capacity to reinforce end-to-end accountability.

II. Enhanced Requirements on App Operators

The Draft Provision strengthens personal information protection obligations of App operators from comprehensive aspects.

(1) Strengthened Informed Consent Requirements

The Draft Provision significantly enhances informed consent obligations, both in form and substance. With respect to access to privacy policies, App operators are now required to provide one-click access to personal information collection and use rules from prominent locations such as the settings page. This requirement goes beyond earlier standards that merely required access within four user interactions, signaling a regulatory shift toward minimizing user effort as an element of effective notice.

Substantively, privacy policies must now include additional information beyond the established "dual list" framework. In particular, App operators must disclose the specific permission names invoked and the frequency of such invocation. The concept of "frequency" is not defined in purely abstract terms; rather, it is linked to concrete usage scenarios, such as continuous location access for navigation functions versus single-instance location access for search or recommendation features. Importantly, this frequency is not determined solely by App-side logic, but is also shaped by operating system behavior and terminal-level frameworks, complicating compliance assessments for App operators.

(2) Additional Technical Requirements to Limit Personal Information Exposure

The Draft Provision introduces explicit technical constraints aimed at reducing unnecessary personal information exposure. Where users choose to upload or send pictures or files, App operators are

required to rely on storage access frameworks provided by intelligent terminals and are prohibited from requesting broad permissions such as access to photo albums, contacts, SMS, or general storage. In practice, this means that Apps must redesign file-handling functions to align with system-level sandbox mechanisms, rather than relying on proprietary interconnections.

The Draft Provision also reinforces the principle that biometric information should not leave the device. Unless otherwise required by law or supported by separate user consent, biometric identifiers such as facial features, fingerprints, and voiceprints must be stored locally on biometric devices and may not be transmitted externally over the internet. This obligation extends the "non-export" principle previously articulated for facial recognition to other forms of biometric data. The requirement for separate consent should be understood as distinct from the initial consent to collect biometric information, indicating that storage or transmission beyond the device constitutes an additional processing purpose requiring heightened user authorization.

(3) Personal Information Deletion and Account Cancellation

In relation to account cancellation, the Draft Provision tightens identity verification requirements by prohibiting App operators from demanding additional personal information—such as facial recognition or photographs of identity documents—beyond what has already been collected, except where genuinely necessary for fraud prevention or security risk control. This reflects regulators' concern that cancellation processes should not become a pretext for further data collection.

The Draft Provision further mandates that account cancellation be completed within fifteen working days, including deletion or anonymization of collected personal information, unless otherwise required by law. While this rule enhances legal certainty, it poses practical challenges. In many sectors, App operators retain certain user data for customer dispute resolution, compliance audits, or reactivation requests. The rigid fifteen-day timeframe may therefore conflict with legitimate business and compliance needs, particularly in highly regulated industries such as finance or insurance.

III. Key Compliance Challenges

Despite its regulatory clarity, the Draft Provision introduces obligations that may be difficult to operationalize.

One major challenge lies in supervising SDK behaviors. App operators are required to adopt "effective technical measures" to audit SDKs' personal information practices, yet the Draft Provision does not specify technical standards or tools. In practice, App operators often lack visibility into SDK source code or runtime behavior, especially where SDKs are deeply embedded or frequently updated. This raises questions as to how App operators can meaningfully fulfill this obligation without industry-wide technical solutions or regulator-endorsed auditing mechanisms.

Another challenge arises from the public consultation requirement imposed on Apps with massive user bases. Apps with more than 50 million registered users or 10 million monthly active users, and with complex business types, must publicly solicit opinions for at least seven working days when materially revising their personal information rules. While intended to enhance transparency and user participation, this requirement may inadvertently force disclosure of sensitive commercial information. Amendments to privacy policies often coincide with the rollout of new functions or changes in technical architecture, and public consultation could reveal business strategies or technical solutions. In practice, the author is sometimes instructed to conduct benchmarking exercises by reviewing competitors' privacy policies and user manuals, amplifying the risk of indirect disclosure.

Finally, the obligation to replace obsolete App versions distributed through authorized channels raises unresolved practical questions. The Draft Provision requires App operators, after releasing updated versions, to ensure replacement of old versions across all authorized distribution channels. It remains unclear whether ordinary online update mechanisms suffice, or whether App operators must take affirmative steps to verify and enforce replacement by each channel. Equally uncertain is how App operators can confirm whether a channel is distributing an App under proper authorization, particularly in the fragmented distribution ecosystems.

Conclusion

The Draft Provision represents a significant step toward systematic, life cycle–based governance of personal information in the App ecosystem. By consolidating fragmented rules, codifying regulatory practice, and extending obligations beyond App operators, it substantially raises compliance expectations. At the same time, the Draft Provision exposes structural tensions between regulatory ambition and technical or commercial realities. Its ultimate effectiveness will depend not only on formal adoption, but also on the issuance of supporting technical standards, enforcement guidance, and industry coordination mechanisms capable of translating legal obligations into operational compliance.

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

Xun Yang
+86 21 3135 8799
xun.yang@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
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

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