Legal Commentary

April 13, 2026

HANKUN
汉坤律师事务所
Han Kun Law Offices

BEIJING | SHANGHAI | SHENZHEN | HONG KONG | HANGZHOU | WUHAN | HAIKOU | SINGAPORE | NEW YORK | SILICON VALLEY

What Changes and What Remains in the Data Protection Obligations for Small-Scale Personal Information Handlers

Authors: Kevin DUAN | Tina WANG | Yi ZOU | Xuechen ZHANG

On April 3, 2026, the Cyberspace Administration of China ("**CAC**") released the Draft Provisions on Simplified Personal Information Protection Measures for Small-Scale Personal Information Handlers (the "**Provisions**") for public comment through May 3, 2026. The draft is significant because it gives concrete regulatory content to Article 62 of the PRC Personal Information Protection Law ("**PIPL**"), which contemplates specialized personal information protection rules and standards for small-scale personal information handlers ("**Small-Scale PI Handler**"). Nearly five years after the PIPL took effect in November 2021, this long-anticipated legislative authorization has finally begun to take shape in operational terms.

From a comparative perspective, the draft reflects a hybrid regulatory approach. **In short, China borrows the numerical data volume threshold of the US CCPA, but applies the targeted obligation-reduction philosophy of the EU GDPR.** Unlike the CCPA, which uses an "exclusionary" model to completely exempt entities that process data for fewer than 100,000 consumers, China uses a "simplification" model. This aligns more closely with the GDPR, which reduces the compliance burden for low-risk entities without removing their fundamental legal obligations. For example, the GDPR exempts organizations with fewer than 250 employees from comprehensive record-keeping and is advancing further simplifications under its 2025 "Digital Omnibus" reforms. China takes a similar path: it preserves the basic framework of the PIPL while introducing itemized simplifications for specific compliance obligations.

How Is a Small-Scale PI Handler Defined?

The Provisions adopt a notably simple definition of a "small-scale personal information handler". Under Article 2, the term refers to a PI Handler that processes the personal information of fewer than 100,000 individuals in China.

While China shares this exact 100,000-person numerical threshold with the CCPA, its test relies solely on data volume. It ignores traditional business metrics such as employee headcount, registered capital, or annual revenue. This differs significantly from the GDPR, which defines small businesses using corporate metrics like employee counts (e.g., fewer than 250 or 750 employees) and revenue caps. It also differs from the CCPA, which considers business activities such as whether an entity derives 50% or

more of its revenue from selling personal information. This makes the Chinese approach relatively straightforward.

In our view, the Provisions are best understood as primarily targeting businesses whose operations remain limited in scale, or whose core business do not center on large-scale personal information processing. For many internet-facing businesses, a user base of 100,000 may be reached relatively quickly, which suggests that the simplified regime may offer meaningful relief mainly during an early-stage growth period rather than on a long-term basis. By contrast, the regime may be more practically relevant to the following enterprises:

- **B2B companies or manufacturing businesses** that process personal information only in ancillary scenarios, such as supplier contact management and visitor registration;
- **Biotech companies and/or small clinics,** with relatively limited data volumes;
- **Standalone stores, hotels, restaurants, and other small offline operators.**

That said, chain operations using a unified brand or centralized system may require closer analysis, as data aggregated across multiple outlets could push the PI Handler above the threshold even where each individual outlet remains small.

The choice of the 100,000-individual threshold is also notable because the same numerical benchmark has already appeared in other PRC data compliance rules, including the exemption threshold under the Regulations on Promoting and Regulating Cross-Border Data Flows and the filing trigger under the Measures for the Security Management of the Application of Facial Recognition Technology. Its recurrence across different legal contexts may suggest a broader regulatory tendency to calibrate certain obligations for processing activities or PI Handlers that are relatively limited in scale and lower in risk, by offering more targeted exemptions or simplified compliance arrangements while preserving the overall structure of the PIPL.

How Do the Provisions Simplify the Compliance Obligations?

Rather than exempting such Small-Scale PI Handlers from the PIPL altogether, the Provisions largely preserve the statute's core framework while introducing targeted simplifications for selected compliance obligations. The following sections examine these adjustments on an obligation-by-obligation basis throughout the lifecycle of personal information processing and internal data compliance management.

I. Transparency Requirements

Under Article 17 of the PIPL, PI Handlers are generally required to provide data subjects with fairly detailed notice regarding their processing activities. In practice, this often leads companies to prepare lengthy privacy policies and make them available through multiple channels. The Provisions would substantially streamline this notice framework for Small-Scale PI Handlers in at least three respects as follows:

1. Simplified Content of the Privacy Notice

Under Article 4, the relevant personal information processing rules need only include: (i) the name of the Small-Scale PI Handler; (ii) the person responsible for handling individuals' rights requests and the relevant contact details; and (iii) the purpose and method of processing, as well as the categories of personal information processed and the retention period.

2. Simplified Form for Displaying the Privacy Notice

Article 4 expressly allows offline businesses to provide notice by posting a notice in a prominent place, while online businesses may incorporate the required notice into user agreements. In addition, Article 6 further provides that publicly posting the privacy notice may substitute for individualized notice in certain circumstances, where (i) the processing does not involve sensitive personal information and is necessary for service provision; and (ii) the handler undertakes neither to provide such information to any third party nor to disclose it publicly.

3. Exemptions from Separate or Repeated Notice

Moreover, the Provisions also dispense with the need to formulate a standalone privacy notice in certain specific scenarios:

- For offline businesses, Article 5 provides that where a Small-Scale PI Handler agrees to comply with the unified personal information processing rules formulated by the relevant service management entity, such as an industrial park, business complex, or commercial property manager, and has been expressly listed in such rules, it need not formulate separate rules of its own.
- For online businesses, Article 8 provides a similar arrangement for merchants operating exclusively through online platforms such as Tmall, Ctrip, Meituan, or Pinduoduo. The merchant may be exempted from repeating the notice obligation if the platform has already fulfilled the notice requirement and the merchant declares its compliance with the platform rules.

These arrangements create reasonable room for small businesses to rely on existing compliance infrastructure and are broadly consistent with how such business models operate in practice. That said, how a Small-Scale PI Handler should effectively make and evidence its declaration of compliance may still need to be clarified through future practice.

Key Bottom Line: Small-Scale PI Handlers must still be able to identify a valid legal basis for processing under Article 13 of the PIPL. The self-assessment audit checklist of the Provisions confirms that the legality of the processing basis remains subject to review, and recent enforcement trends likewise show that unauthorized collection or use of personal information continues to be a priority issue for regulators. The Provisions therefore simplify compliance mechanics, but not the basic requirement that processing must be lawful from the outset.

II. Consent for Sensitive Personal Information Processing

Under the PIPL, the processing of sensitive personal information is subject to a heightened compliance standard. Regulators have also issued national standards to further guide processing practices in this area, reflecting the consistently higher compliance expectations attached to sensitive personal information. As a result, Article 10 of the Provisions introduces only a limited simplification.

The main practical relaxation appears to be that, where an individual voluntarily provides sensitive personal information such as facial information or biological samples in an informed manner, the handler may process such information in accordance with the disclosed purpose, method and categories of processing, without going through an additional standalone consent formality.

This requirement is also broadly consistent with the approach reflected in the national standards, i.e., Information Security Technology–Implementation Guidelines for Notices and Consent in Personal Information Processing (GB/T 42574-2023) and Data Security Technology–Security Requirements for Processing of Sensitive Personal Information (GB/T 45574-2025), both of which recognize effective consent where the individual actively provides the relevant sensitive personal information after adequate notice. Nevertheless, in our view, this is best understood as a narrow facilitation for cases of active provision by the individual, rather than a general dilution of the compliance threshold for sensitive personal information.

Key Bottom Line: The compliance bottom line for sensitive personal information remains largely unchanged. Outside the limited scenario described above, PI Handlers should still proceed on the basis that the stricter PIPL requirements continue to apply: Article 28 requires that such processing must serve a specific purpose and be supported by sufficient necessity; Articles 38 and 39 impose additional requirements where sensitive personal information is transferred overseas; and Article 55 requires a personal information protection impact assessment ("PIPIA").

In practice, we believe this suggests that small businesses should remain cautious about collecting sensitive personal information without users' knowledge or awareness, for example, by passively recording device location data in the background to track users' movements.

III. Security Assessment Procedures for Cross-Border Data Transfers

In the area of cross-border transfers of personal information, which has long been subject to heightened regulatory scrutiny in China, the Provisions mainly offer procedural simplifications. Under the existing data export regime, where a PI Handler is required to undergo a data export security assessment, the application must be submitted through the provincial-level cyberspace administration to the central CAC. Under the Provisions, the provincial authority may conduct a completeness review of the application materials and form an assessment conclusion, which would be submitted to the CAC for approval. This could help shorten the overall review timeline. The Provisions also contemplate supportive measures at the local level, including guidance from local authorities and data export service centers on relevant compliance issues.

Key Bottom Line: Apart from these procedural simplifications, the Provisions do not alter the existing exemption thresholds or applicability criteria for cross-border data transfer. Small-Scale PI Handlers must still determine whether a security assessment, standard contractual clauses, or another applicable transfer mechanism is required under the existing rules. Nor do the Provisions displace the baseline obligations that continue to apply to personal information exports under the PIPL and related regulations, including the duties to provide detailed notice, obtain separate consent where required, and conduct a PIPIA.

IV. PIPIA and PI Audits

Under the PIPL, PI Handlers are required to conduct both PIPIA and personal information protection compliance audits ("**PI Audit**"). Regulators have also issued implementing rules (e.g., the Measures for the Administration of Personal Information Protection Compliance Audits, "**PI Audit Measures**") and national standards (e.g., Information Security Technology–Guidelines for Personal Information Security Impact Assessment (GB/T 39335-2020)) to guide such activities. These frameworks typically involve multiple assessment dimensions and relatively complex procedures.

In this context, the Provisions introduce simplified templates and processes, thereby reducing both the operational complexity and compliance costs associated with such assessments.

1. Simplified PI Audit Procedures and Clarified Timing Requirements

Pursuant to Article 14 of the Provisions, a Self-Assessment Checklist for Personal Information Protection Compliance Audits for Small-Scale Personal Information Handlers (Annex 1) is introduced. This checklist requires Small-Scale PI Handlers to tick off compliance for only 24 audit items and to provide explanations for any non-compliance along with corresponding remediation measures, which significantly reduces the complexity and burden of the audit process.

Under the PI Audit Measures, PI Handlers processing the personal information of more than 10 million individuals are required to conduct a compliance audit at least once every two years, while there was no explicit timing requirement for other PI Handlers. Article 14 of the Provisions now clarifies that Small-Scale PI Handlers are required to conduct a PI Audit once every five years and retain the self-assessment checklist for at least five years. Compared to the previous regulatory ambiguity, this provides a clearer compliance timeline.

2. Simplified PIPIA Requirements

Article 15 of the Provisions also provides a simplified approach to conducting PIPIAs through a standardized Personal Information Protection Impact Assessment Form for Small-Scale Personal Information Handlers (Annex 2). Under this approach, Small-Scale PI Handlers are only required to record the conclusions of the assessment, thereby reducing procedural burden and operational costs. The impact assessment form shall be retained for at least three years.

3. Exemptions from PIPIA and PI Audit

The Provisions introduce certain exemption scenarios to avoid duplicative compliance efforts:

- Under Article 8, Small-Scale PI Handlers operating on internet platforms may rely on the platform's completed PI Audit and PIPIA, and are not required to conduct separate assessments themselves.
- Under Article 18, Small-Scale PI Handlers that have obtained personal information protection certification may be exempted from conducting PI Audit during the validity period of such certification.

V. Data Compliance Management and Incident Response Mechanisms

1. Simplification of Internal Personal Information Protection Policies

Under the PIPL, PI Handlers are generally required to establish internal management systems and operating procedures for personal information protection. To ease that burden, Article 16 of the Provisions provides that Small-Scale PI Handlers are no longer required to maintain a dedicated standalone regime for this purpose. Instead, they may adopt a more flexible approach by incorporating personal information protection rules and incident response measures into their existing internal policies and management documents, thereby reducing the cost and administrative effort associated with developing and maintaining a separate compliance framework.

That said, this simplification relates only to form rather than substance. Small-Scale PI Handlers are still required to define internal management requirements for personal information processing activities based on factors such as processing purpose, processing methods, types of personal information, impact on individuals' rights and interests, and potential security risks. These internal rules shall ensure compliance with applicable laws and administrative regulations, and shall effectively prevent unauthorized access, as well as personal information leakage, tampering, or loss.

2. Simplification of Data Incident Response

With respect to personal information security incident response, Article 17 of the Provisions allows for more flexible notification methods where notification to individuals is required, including:

- posting a notice in a prominent location for offline businesses; or
- using pop-up notifications for online products.

Compared to Article 11 of the Regulations on the Administration of Network Data Security, which contemplates notification through methods such as telephone, SMS, instant messaging, email, or public announcements, the Provisions significantly reduce the operational burden associated with individual notifications.

Despite the simplified format, the legal obligations for Small-Scale PI Handlers to promptly take remedial measures, report to the relevant regulatory authorities, and notify affected individuals remain unchanged. The specific content required in reports to regulators may refer to provisions such as the Measures for the Administration of National Cybersecurity

Incident Reporting.

For notifications to individuals, as required under the PIPL, the notice shall still include:

- ***the types of personal information affected and the cause and potential harm of the incident;***
- ***remedial measures taken by the handler and measures individuals may take to mitigate harm; and***
- ***the contact details of the handler.***

VI. Termination of Services and Personal Information Processing

Under the PIPL, where a PI Handler ceases to provide products or services, it is required to proactively delete the relevant personal information. Also, in the context of transfers of personal information resulting from dissolution, split-up, merger, bankruptcy or similar corporate changes, notice shall be provided to individuals, and the successor shall obtain consent from the personal information subjects where necessary. The Provisions streamline the compliance burden on Small-Scale PI Handlers in service termination scenarios by easing notification and data deletion obligations.

1. Simplified Notice Requirements

Under Article 9 of the Provisions, individualized notice may be replaced with a unified public announcement, with separate arrangements for offline and online scenarios: offline businesses may provide notice by posting an announcement on site, while online businesses may do so through a pop-up announcement on the relevant user interface.

However, such announcements must meet specified timing requirements. Specifically, the announcement must be made at least 30 working days in advance and remain publicly available for no less than 30 working days.

2. Guidance in Data Deletion

Acknowledging the difficulties for Small-Scale PI Handlers to implement the data deletion requirements under the PIPL, the Provisions introduce a more practical approach by offering guidance from administrative authorities.

Article 9 provides that where a handler genuinely lacks the capability to delete personal information, it may report to the competent local authority and request assistance. Where the competent authority is unclear, the handler may report to the competent municipal-level cyberspace administration.

VII. Administrative Penalties

The Provisions are designed to facilitate secure and efficient personal information processing by Small-Scale PI Handlers, and this policy orientation is also reflected in a more lenient administrative enforcement approach aimed at fostering an inclusive business environment for small and micro enterprises.

Article 19 specifies **circumstances under which no administrative penalty will be imposed**, including where the violation is minor, corrected in a timely manner, and does not result in harmful consequences, as well as cases of first-time violations with minor harm that are promptly rectified.

Article 20 further sets out **circumstances for mitigation or reduction of penalties**, including:

- proactively eliminating or mitigating the harmful consequences of the violation;
- voluntarily disclosing violations not yet identified by the competent authorities;
- promptly notifying individuals, taking remedial measures, and proactively reporting to authorities in the event of a personal information security incident;
- demonstrating meritorious cooperation in assisting authorities with enforcement actions; and
- other circumstances warranting leniency or mitigation in accordance with law.

That said, it should be emphasized that mitigation or exemption from administrative penalties does not equate to exemption from liability. Small-Scale PI Handlers shall still implement appropriate safeguards for the protection of individuals' rights and interests, as well as corresponding security management measures, taking into account the nature and scope of their data processing activities.

****

Annex 1 Self-Assessment Checklist for Personal Information Protection Compliance Audits for Small-Scale Personal Information Handlers

Annex 2 Personal Information Protection Impact Assessment Form for Small-Scale Personal Information Handlers

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Kevin DUAN

Tel: +86 10 8516 4123
Email: kevin.duan@hankunlaw.com