A Quick 7-Step Guide to Complete a Minor Personal Information Protection Compliance Audit

By Xun Yang | Roy Zheng

On the evening of 29 December 2025, the eve of the new year, the Cyberspace Administration of China (CAC) issued an announcement requiring "all entities that process minors' personal information" to log on to the "Personal Information Protection Business System" and complete the on-line filing of their previous-year minor personal information compliance-audit status no later than 31 January 2026. There is no pilot programme and no grace period; the minor-specific audit that could originally be "put off until next year" has been pulled into the here-and-now.

From that moment on, the question we have been asked most often are:

"Is our company actually required to conduct a minors-specific compliance audit?"
"Do we have to complete the filing by January 31?"
"Given that this obligation is mandatory, how can we finish a dedicated audit on minors' personal information protection within such a tight timeframe?"

I. Minor Personal Information Protection Compliance Audit

A personal information protection compliance audit (PIPCA) is a statutory obligation under the Personal Information Protection Law (PIPL). Every personal information processor must conduct PIPCA on a regular basis. Where minors' data are involved, the sensitivity of the data subjects triggers a higher requirement: Article 37 of the Regulations on the Online Protection of Minors stipulates that "anyone who processes minors' personal information shall conduct a specialised compliance audit on minors personal information protection every year". The audit method is the same as for ordinary PIPCA and is governed by the Measures for Personal Information Protection Compliance Auditing and its annex, the Audit Guidelines.

如果您需要本出版物的中文本,

Publication@llinkslaw. com

For more Llinks publications, please contact:

Publication@llinkslaw.com

Apart from meeting the legal requirement, conducting the audit brings three benefits:

(1) Full-system health check. Personal information protection obligations run through procurement, production, sales, management, HR and every other business link. An audit systematically maps personal-data processing activities, identifies risks early and prevents small issues from becoming material violations.
(2) Proof of innocence. In disputes, PIPL Article 69 applies a presumption of fault: once a processing activity is alleged to be infringing, the enterprise must prove it was not at fault or else bear liability. A third-party audit report is objective evidence that can rebut the claim and lower the probability of being held responsible.
(3) Stronger market competitiveness. The market is paying ever more attention to data compliance. In procurement, insurance, reinsurance and other transactions, partners often treat personal information protection abilities as a screening criterion. Complete audit records enhance corporate credibility and directly increase the likelihood of winning business and commanding a premium.

From the regulator's point of view, requiring companies to file by 31 January serves two purposes: first, as a supervisory tool to implement the statutory obligation; second, to use the self-submitted reports as a basis for mapping minors' data processing and for later enforcement.

II. Practical Questions on Carrying Out the Audit

Now that we know the audit is mandatory and beneficial, we must decide when and how to do it.

Q1. Is any entity that process minors' data required to conduct audit?

Strictly speaking, even an occasional or small-scale processing of minors' data triggers the obligation to conduct the specialised audit and to report on-line.

The obligation originates in the Regulations on the Online Protection of Minors, whose scope is broad: on-line product and service providers, personal-data processors, and manufacturers/sellers of smart-terminal products are all covered. Any processing of minors' data is captured. In practice, however, regulatory attention focuses on:

- Internet products or services aimed at minors—on-line games, on-line education, etc.;
- Scenarios that collect or process minors' data as the main or sole group, e.g. insurance where the insured or beneficiary is a minor;
- Businesses that inevitably include minors, e.g. children's smart-watches or home-security cameras with facial recognition.

Q2. Must processors that handle only a tiny amount of minors' data still conduct audit and report?

Yes. The law grants no de-minimis exemption. Unlike outbound-data assessments—which I predicted would see their thresholds lowered because regulators could never review thousands of them—personal information protection compliance audits use a self-reporting model: companies conduct the audit themselves and the government does not review each one individually. This greatly reduces the regulatory burden, but it also means the obligation applies to every processor, however small the volume.

Still, volume (or, more precisely, the weight of minors' data in the business) matters, because purely incidental processing of a handful of records is unlikely to be a regulatory priority.

Q3. How do we select the scenarios to audit?

In theory every scenario that involves minors' data must be covered. That does not mean equal effort should be spent on each one. A comprehensive scope satisfies the legal requirement and prevents omissions being discovered later, but you should also identify the high-risk scenarios and focus your time and resources there. This aligns with the Cyber-Security Law's requirement to classify information by importance and with the principle of dynamic compliance, and it prevents regulators from being overwhelmed by a flood of low-risk disclosures.

Factors to consider include:

- Nature of the service/product: is it aimed at minors?
- Volume and importance: how many minors' records are processed, and what share of the total do they represent? Is processing occasional or inevitable?
- Sensitivity of the data: health, home address, location history, etc., rather than just name and school.

Q4. What audit points should we check?

We have distilled more than 50 audit points from past engagements. In theory the minor-specific audit should cover the whole life-cycle and all 50 points, but within one month an unfocused full-scope audit is neither practical nor what regulators need.

Pick the points that matter for the specific scenario and for minors:
Collection: is parental consent obtained for U14?
Use: is the minor unfairly profiled by age for personalised recommendations or automated decisions?
Storage: are special safeguards defined for minors' data in this scenario?
Transfer: Have encryption measures been adopted for data transmission?

Industry specific points include:

- On-line games: real-name authentication, in-game purchases, and how data are shared with SDKs during identity checks.
- Insurance: underwriting where the insured is a minor, retention of guardian-relationship proof, security of minors' images, disclosure obligations.

- Funds: verification of guardian/inheritance relationships when minors inherit shares, legality and necessity of supporting documents, and their secure retention.
- In all cases, how the system distinguishes adults from minors is itself a key audit point.

III. One-Month "Seven-Step" Sprint

31 January is not literally a life-or-death line, but companies should still aim to finish the audit and file by then.

Step 1 Launch immediately

Use the regulatory notice as the trigger. Like any personal information protection compliance audit, the project needs Legal, Compliance, IT, Business, HR and other departments. External counsel can accelerate the work and keep it market-standard.

Step 2 Merge similar tasks

Re-use questionnaires and evidence pools already built for "data-outbound risk self-assessment", "personal-data protection impact assessment (PIA)", etc. Avoid re-inventing the wheel and save time.

Step 3 Map the high-risk scenarios

Based on your business and the principles above, pick the scenarios that collect or process minors' data in sensitive ways; concentrate time and resources there to satisfy regulatory expectations.

Step 4 Build a "minor-data protection" checklist

For each high-risk scenario, list the key audit points and the exact documents or evidence required, so business teams know what to hand over. In past audits we found that most delay occurs while we coach business units to produce processing records and evidence. Business staff often do not know which internal document matches which legal term. To reduce that friction we have prepared industry-specific checklists for on-line gaming, insurance brokerage and fund management that spell out, point by point, which files and data are needed. These streamlined templates can shorten the evidence-gathering phase dramatically.

Step 5 Audit + freeze evidence

Use walk-through testing and other audit methods. Given the tight timetable, focus on capturing the principal evidence for each processing step involving minors' data.

Step 6 Issue the report

A regulatory-purpose report can be concise, referencing only laws, regulations and rules. Recommendations that cite national standards or industry best practice can wait for the full-scope audit later.

Step 7 File on-line

Log on to https://grxxbh.cacdtsc.cn and complete the filing as required.

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