

Personal Information Protection Compliance Audit Measures of the PRC

Dan Young Business Consultancy — www.danyoungcpa.com

Unofficial English translation prepared for reference only. The official Chinese text prevails.

Issued by the Cyberspace Administration of China on February 12, 2025

Effective: May 1, 2025

Article 1 — These Measures are formulated in accordance with the Personal Information Protection Law of the People's Republic of China, the Regulations on the Administration of Network Data Security, and other relevant laws and administrative regulations, for the purposes of regulating personal information protection compliance audit activities, protecting personal information rights and interests, and promoting the lawful, rational and effective use of personal information.

Article 2 — These Measures apply to compliance audits conducted in respect of personal information processing activities carried out within the territory of the People's Republic of China.

Article 3 — For the purposes of these Measures, a “personal information protection compliance audit” (hereinafter a “compliance audit”) means the activity of reviewing, evaluating and supervising whether the personal information processing activities of a personal information processor comply with the provisions of laws and administrative regulations.

Article 4 — A personal information processor that processes the personal information of more than 10 million individuals shall conduct a compliance audit at least once every two years.

Article 5 — Under any of the following circumstances, the Cyberspace Administration of China and other relevant competent authorities may require a personal information processor to commission a professional institution to conduct a compliance audit of its personal information processing activities:

- (1) where the personal information processing activities are found to present a relatively high risk, or a personal information security incident has occurred;
- (2) where the personal information processing activities are likely to harm the rights and interests of a large number of individuals; or
- (3) where a public interest lawsuit concerning personal information protection has been initiated, or complaints and reports filed by relevant organizations or individuals have been verified and reflect that problems exist in the personal information processing activities.

Article 6 — A professional institution conducting compliance audits shall possess the capabilities corresponding to the conduct of personal information protection compliance audits, and shall have a sound system for the management of audit work and appropriate safeguards for independence and confidentiality.

Article 7 — A personal information processor that conducts a compliance audit pursuant to these Measures shall commission a professional institution to carry out the audit. The professional institution shall conduct the compliance audit independently and objectively, and shall not be subject to undue interference from the personal information processor.

Article 8 — A compliance audit shall examine, among other matters, whether the personal information processor has a lawful basis for processing personal information and whether the processing falls within the scope necessary for the stated purpose.

Article 9 — A compliance audit shall examine whether the personal information processor has formulated and made public its personal information processing rules, and whether it has fulfilled its obligation to notify individuals of the items set out in the Personal Information Protection Law.

Article 10 — A compliance audit shall examine whether the personal information processor has obtained the separate or written consent of individuals where such consent is required by laws and administrative regulations, and whether individuals may withdraw their consent in a convenient manner.

Article 11 — A compliance audit shall examine whether the processing of sensitive personal information complies with the specific purposes and adequate necessity requirements prescribed by law, whether separate consent has been obtained, and whether the special provisions on the processing of personal information of minors under the age of fourteen have been observed.

Article 12 — A compliance audit shall examine whether the personal information processor has entered into agreements with entrusted parties, and whether it has complied with the requirements governing the joint processing, entrustment of processing, and provision of personal information to other processors.

Article 13 — A compliance audit shall examine whether the provision of personal information outside the territory of the People's Republic of China has satisfied the conditions prescribed by law, including the completion of the necessary security assessment, certification, or conclusion of a standard contract.

Article 14 — A compliance audit shall examine whether the use of personal information to conduct automated decision-making has complied with the provisions on transparency, fairness and impartiality, and whether the rights of individuals in respect of automated decision-making have been protected.

Article 15 — A compliance audit shall examine whether the personal information processor has adopted appropriate technical and organizational security measures, such as encryption and de-identification, in accordance with the purpose of processing and the security risks involved.

Article 16 — A compliance audit shall examine whether the personal information processor has, as required by law, designated a person responsible for personal information protection, established internal management systems and operating procedures, conducted training, and carried out other compliance management obligations.

Article 17 — A compliance audit shall examine whether the personal information processor has carried out personal information protection impact assessments where required by law, and whether it has fulfilled its obligations to monitor risks and to notify and report in the event of a personal information security incident.

Article 18 — A compliance audit shall examine whether the personal information processor has provided individuals with convenient channels for exercising their rights to access, copy, correct, supplement and delete their personal information, and whether it has honored requests for such exercise in a timely manner.

Article 19 — A compliance audit shall examine such other matters as are required by laws and administrative regulations in connection with personal information processing activities.

Article 20 — Upon completion of a compliance audit, the professional institution shall issue an audit report. The audit report shall state the scope and content of the audit, the problems identified, the conclusions of the audit, and the recommendations for rectification.

Article 21 — Where a compliance audit identifies problems in personal information processing activities, the personal information processor shall carry out rectification in a timely manner and, where the audit was conducted at the request of the Cyberspace Administration of China or other competent authorities, report the rectification situation to the requesting authority within the prescribed time limit.

Article 22 — A professional institution and its personnel shall keep confidential any state secrets, trade secrets and personal information obtained in the course of the compliance audit, and shall not disclose or use such information except for the purpose of the audit or as required by law.

Article 23 — Where a personal information processor refuses to cooperate with a compliance audit required under these Measures, or obstructs or hinders such audit, the Cyberspace Administration of China and other competent authorities shall handle the matter in accordance with the Personal Information Protection Law of the People's Republic of China and other laws and administrative regulations.

Article 24 — Where a professional institution issues a false audit report or fails to conduct the audit in accordance with the relevant requirements, the Cyberspace Administration of China and other competent authorities shall handle the matter in accordance with the law.

Article 25 — Where state organs process personal information for the performance of their statutory duties, the compliance audit of such processing shall be carried out in accordance with the relevant provisions of laws and administrative regulations.

Article 26 — These Measures shall come into force on May 1, 2025.

Disclaimer: This English translation is provided for reference and general informational purposes only. It is not an official translation and may not reflect subsequent amendments or interpretations. In the event of any discrepancy, the original Chinese text shall prevail. This translation does not constitute legal advice, and readers should consult a qualified legal professional for matters affecting their rights or obligations.