Annex1

Checklist for Personal Information Protection Compliance Audits for Small-Scale Personal Information Processors

No.	Compliance Audit Items	Self-Inspection of Compliance Status	Description of Non-compliance and Rectification
1	When conducting a compliance audit on the legal basis for personal information processing activities, the following items shall be the focus of examination: (1) Where personal information is processed based on personal consent, whether such consent has been obtained, and whether the consent was given voluntarily and explicitly by the individual on the premise of being fully informed; (2) Where personal information is processed based on personal consent, if the purpose, manner, or type of personal information being processed changes, whether consent has been re-obtained from the individual; (3) Where personal information is processed based on personal consent, whether separate consent or written consent has been obtained from the individual in accordance with laws and administrative regulations; (4) Where personal information is processed without obtaining personal consent, whether such processing falls within the circumstances stipulated by laws and administrative regulations where personal consent is not required.	☐Compliant ☐Non-compliant ☐Not Applicable	
2	When conducting a compliance audit on personal information processing rules, the following items shall be the focus of examination: (1) Whether the name and contact information of the personal information processor have been truthfully, accurately, and completely disclosed; (2) Whether the personal information collected, along with its processing methods and categories, has been set out in an easily accessible format such as a list; (3) Whether the processing is directly related to the processing purpose and conducted in a manner with the least impact on the rights and interests of individuals; (4) Whether the retention period of personal information, or the method for determining the retention period, the processing method upon expiry, and the determination of the minimum retention period necessary to achieve the processing purpose have been clearly specified;	☐Compliant ☐Non-compliant ☐Not Applicable	

	(5) Whether the channels and methods for individuals to access, copy, transfer, correct, supplement, delete, restrict the processing of personal information, cancel accounts, and withdraw consent have been clearly specified.		
3	When conducting a compliance audit on the personal information processor's fulfillment of the obligation to notify individuals of personal information processing rules, the following items shall be the focus of examination: (1) Prior to processing personal information, whether the personal information processor has truthfully, accurately, and completely notified individuals of the personal information processing rules in a prominent manner and in clear, easily understandable language; (2) Whether the size, font, and color of the notification text facilitate an individual's complete reading of the notified matters; (3) Whether offline notification fulfills the notification obligation to individuals through various methods such as labeling and explanatory notes; (4) Whether online notification provides textual information or fulfills the notification obligation to individuals through appropriate means; (5) Where the personal information processing rules are changed, whether the changes have been promptly notified to individuals; (6) Where notification is not required for personal information processing, whether such non-notification falls within the circumstances stipulated by laws and administrative regulations where confidentiality is required or notification is not necessary.	☐Compliant ☐Non-compliant ☐Not Applicable	
4	When conducting a compliance audit on the joint processing of personal information by a personal information processor with other personal information processors, the following items shall be the focus of examination: (1) Whether the respective rights and obligations of each party have been agreed upon; (2) The mechanism for protecting the rights and interests relating to personal information; (3) The reporting mechanism for personal information security incidents; (4) Other rights and obligations required to be agreed upon under laws and administrative regulations.	☐Compliant ☐Non-compliant ☐Not Applicable	
5	When conducting a compliance audit on the entrustment of personal information processing by a personal information processor, the following items shall be the focus of examination: (1) Prior to entrusting the processing of personal information, whether the personal information processor has conducted a personal information protection impact assessment; (2) In the contract entered into between the personal information processor and the entrusted party, whether the purpose, duration, methods, categories of personal information, protective measures, and the rights and obligations of both parties for the entrusted processing have been agreed upon with the entrusted party; (3) Whether the personal information processor has adopted periodic inspections or other measures to supervise the personal information processing activities of the entrusted party.	☐Compliant ☐Non-compliant ☐Not Applicable	

6	Where a personal information processor needs to transfer personal information due to a merger, reorganization, division, dissolution, declaration of bankruptcy, or other such reasons, the focus of examination shall be whether the personal information processor has notified individuals of the name and contact information of the recipient.	☐Compliant ☐Non-compliant ☐Not Applicable	
7	When conducting a compliance audit on a personal information processor's provision of personal information it processes to other personal information processors, the following items shall be the focus of examination: (1) Where personal information is processed based on personal consent, whether separate consent of the individual has been obtained; (2) Whether individuals have been notified of the name, contact information, processing purpose, processing method, and categories of personal information of the recipient, except where laws and administrative regulations require confidentiality or notification is not necessary; (3) Whether a personal information protection impact assessment has been conducted in advance.	☐Compliant ☐Non-compliant ☐Not Applicable	
8	When conducting a compliance audit on a personal information processor's use of automated decision-making to process personal information, the following items shall be the focus of examination: (1) The transparency of automated decision-making, and whether the results of automated decision-making are fair and impartial; (2) Whether individuals have been notified in advance of the categories of personal information processed through automated decision-making and the potential impacts thereof; (3) Whether a personal information protection impact assessment has been conducted in advance; (4) Whether a guarantee mechanism has been provided to users to enable individuals to refuse, through convenient means, decisions made by automated decision-making that have a significant impact on the rights and interests of individuals, and to require the personal information processor to provide an explanation of decisions made by automated decision-making that have a significant impact on the rights and interests of users; (5) When conducting information push notifications or commercial marketing to individuals, whether options not targeted to individual characteristics have been simultaneously provided, or whether a convenient means to refuse automated decision-making services has been provided; (6) Whether effective measures have been taken to prevent automated decision-making from imposing unreasonable differential treatment on individuals in transaction terms based on consumer preferences, transaction habits, or similar factors; (7) Other matters that may affect the transparency and fairness and impartiality of automated decision-making results.	☐Compliant ☐Non-compliant ☐Not Applicable	
9	When conducting a compliance audit on a personal information processor's disclosure of personal information based on personal consent, the following items shall be the focus of examination: (1) Prior to disclosing personal information it processes, whether the personal information processor has obtained separate consent of the individual, whether such authorization is genuine and valid, and whether there are any	☐Compliant ☐Non-compliant ☐Not Applicable	

	instances of disclosing personal information against the individual's wishes; (2) Prior to disclosing personal information, whether the personal information processor has conducted a personal information protection impact assessment.		
10	Where a personal information processor installs image collection or personal identification devices in public places, the focus of examination shall be on the legality of installing such image collection and personal identification devices and the purposes for which the collected personal information is used. The examination shall include, but is not limited to: (1) Whether the installation is necessary for maintaining public security, and whether the collected personal information is processed for commercial purposes; (2) Whether conspicuous warning signs have been set up; (3) Where the personal images and identification information collected by the personal information processor are used for purposes other than maintaining public security, whether separate consent of the individual has been obtained.	☐Compliant ☐Non-compliant ☐Not Applicable	
11	When conducting a compliance audit on a personal information processor's processing of publicly disclosed personal information, the focus of examination shall be on whether the personal information processor engages in any of the following unlawful or non-compliant acts: (1) Sending commercial information unrelated to the purpose of disclosure to email addresses, mobile phone numbers, or other contact details contained in publicly disclosed personal information; (2) Using publicly disclosed personal information to engage in cyberbullying, spreading online rumors and false information, or other similar activities; (3) Processing publicly disclosed personal information that an individual has explicitly refused to have processed; (4) Having a significant impact on the rights and interests of individuals without obtaining personal consent; (5) Collecting, retaining, or processing publicly disclosed personal information to an extent, duration, or for purposes that exceed a reasonable scope.	☐Compliant ☐Non-compliant ☐Not Applicable	
12	When conducting a compliance audit on a personal information processor's processing of sensitive personal information, the following items shall be the focus of examination: (1) Where personal information is processed based on personal consent, for the processing of sensitive personal information such as biometric identification, religious beliefs, specific identity, medical and health information, financial accounts, and location tracking, whether separate consent of the individual has been obtained in advance; (2) Where personal information is processed based on personal consent, for the processing of personal information of minors under the age of fourteen, whether consent has been obtained in advance from the parents or other guardians of the minor; (3) Whether the purpose, manner, and scope of processing sensitive personal information are lawful, legitimate, and necessary;	☐Compliant ☐Non-compliant ☐Not Applicable	

	(4) Whether a personal information protection impact assessment has been conducted in advance; (5) Whether individuals have been notified of the necessity of processing sensitive personal information and the impact on the rights and interests of individuals, except where laws and administrative regulations require confidentiality or notification is not necessary; (6) Where written consent is required under laws and administrative regulations, whether written consent has been obtained; (7) Whether the restrictive provisions of laws and administrative regulations on the processing of sensitive personal information have been complied with.		
13	When conducting a compliance audit on a personal information processor's processing of personal information of minors under the age of fourteen, the following items shall be the focus of examination: (1) Whether dedicated personal information processing rules have been formulated; (2) Whether minors and their guardians have been notified of the purpose, manner, and necessity of processing the minor's personal information, as well as the categories of personal information processed and the protective measures taken, except where laws and administrative regulations provide that notification is not required; (3) Where personal information is processed based on personal consent, whether there are any acts of coercing minors or their guardians into consenting to the processing of non-essential personal information.	☐Compliant ☐Non-compliant ☐Not Applicable	
14	When conducting a compliance audit on a personal information processor's provision of personal information to overseas recipients, the following items shall be the focus of examination: (1) Whether critical information infrastructure operators have passed the security assessment organized by the national cyberspace administration authority when providing personal information to overseas recipients, unless otherwise provided by laws, administrative regulations, or the national cyberspace administration authority; (2) Whether data processors other than critical information infrastructure operators that have cumulatively provided, from January 1st of the current year, personal information of more than 1,000,000 individuals (excluding sensitive personal information) or sensitive personal information of more than 10,000 individuals to overseas recipients have passed the security assessment organized by the national cyberspace administration authority, unless otherwise provided by laws, administrative regulations, or the national cyberspace administration authority; (3) Whether data processors other than critical information infrastructure operators that have cumulatively provided, from January 1st of the current year, personal information of more than 100,000 individuals but fewer than 1,000,000 individuals (excluding sensitive personal information) or sensitive personal information of fewer than 10,000 individuals to overseas recipients have, in accordance with the provisions of the national cyberspace administration authority, passed personal information protection certification, or have entered into a contract with the overseas recipient in accordance with the standard contract formulated by the national cyberspace administration authority and filed with the provincial-level cyberspace administration authority of the locality, or have met other conditions stipulated by laws, administrative regulations, or the national cyberspace administration	☐Compliant ☐Non-compliant ☐Not Applicable	

	authority; (4) Where there are circumstances involving the provision of personal information stored within the territory of the People's Republic of China to foreign judicial or law enforcement authorities, whether approval from the competent authorities of the People's Republic of China has been obtained; (5) Whether personal information has been provided to organizations or individuals that have been placed on the list of restricted or prohibited personal information recipients.		
15	When conducting a compliance audit on the protection of the right to erasure of personal information, the following items shall be the focus of examination: (1) Whether the purpose of personal information processing has been achieved, cannot be achieved, or is no longer necessary for achieving the processing purpose; (2) Whether the personal information processor has ceased to provide products or services, or whether the individual has cancelled their account; (3) Whether the retention period has expired; (4) Whether the individual has withdrawn consent; (5) Whether the personal information processor has processed personal information in violation of laws or administrative regulations or in breach of agreement; (6) Where personal information should be deleted but the retention period stipulated by laws and administrative regulations has not expired, or where the deletion of personal information is technically difficult to implement, whether the personal information processor has ceased all processing other than storage and the adoption of necessary security measures.	☐Compliant ☐Non-compliant ☐Not Applicable	
16	When conducting a compliance audit on a personal information processor's protection of individuals' rights in personal information processing activities, the following items shall be the focus of examination: (1) Whether a convenient mechanism for receiving and processing requests for individuals to exercise their rights has been established; (2) Whether requests from individuals to exercise their rights have been responded to in a timely manner, and whether the processing opinion or execution results have been communicated in a timely, complete, and accurate manner; (3) Where a request from an individual to exercise their rights is refused, whether reasons have been provided to the individual.	☐Compliant ☐Non-compliant ☐Not Applicable	
17	Personal information processors shall respond to requests from individuals and provide explanations of their personal information processing rules. During compliance audits, the following shall be the focus of evaluation: (1) Whether the personal information processor provides convenient methods and channels to receive and handle requests from individuals for explanations of personal information processing rules; (2) Upon receiving a request from an individual, whether the personal information processor provides an	☐Compliant ☐Non-compliant ☐Not Applicable	

	explanation of its personal information processing rules within a reasonable time using plain and easily understandable language.		
18	Personal information processors shall formulate internal management systems and operating procedures in accordance with the provisions of laws and administrative regulations, clarify organizational structure and job responsibilities, establish work processes, and improve internal control systems to ensure the compliance and security of personal information processing. During compliance audits, the focus shall be on examining the personal information processor's internal management systems and operating procedures for personal information protection, including but not limited to: (1) Whether the policies, objectives, and principles of personal information protection work comply with the provisions of laws and administrative regulations; (2) Whether the organizational structure, staffing, code of conduct, and management responsibilities for personal information protection are commensurate with the personal information protection responsibilities that should be fulfilled; (3) Whether personal information has been classified according to its categories, sources, sensitivity levels, purposes, and other relevant factors; (4) Whether an emergency response mechanism for personal information security incidents has been established; (5) Whether a personal information protection impact assessment system and a compliance audit system have been established; (6) Whether a smooth complaint and reporting process for personal information protection has been established; (7) Whether operational permissions for personal information processing have been reasonably formulated; (8) Whether a security education and training plan for personal information protection has been formulated and implemented; (9) Whether a performance evaluation system for the Personal Information Protection Officer and relevant personnel has been established; (10) Whether an accountability system for unlawful personal information processing has been established; (11) Other matters stipulated by laws and administrative regulations.	☐Compliant ☐Non-compliant ☐Not Applicable	
19	Personal information processors shall adopt security technical measures commensurate with the scale and types of personal information they process, and shall evaluate the effectiveness of the technical measures adopted by the personal information processor. The evaluation shall include, but is not limited to: (1) Whether appropriate security technical measures have been adopted to achieve the confidentiality, integrity, and availability of personal information; (2) Whether security technical measures such as encryption and de-identification have been adopted to ensure that the identifiability of personal information is eliminated or reduced without the use of additional information; (3) Whether the security technical measures adopted can reasonably determine the operational permissions of	☐Compliant ☐Non-compliant ☐Not Applicable	

	relevant personnel for accessing, copying, and transmitting personal information, thereby reducing the risk of unauthorized access and misuse of personal information during processing.		
20	When conducting a compliance audit on the formulation and implementation of the personal information processor's education and training plan, the following shall be the focus of evaluation: (1) Whether the relevant security education and training have been provided as planned to management personnel, technical personnel, operational personnel, and all staff, and whether the personal information protection awareness and skills of relevant personnel have been assessed; (2) Whether the training content, methods, target audience, frequency, and other factors can meet the needs of personal information protection.	☐Compliant ☐Non-compliant ☐Not Applicable	
21	When conducting a compliance audit on the performance of duties by the Personal Information Protection Officer designated by the personal information processor, the following items shall be the focus of examination: (1) Whether the Personal Information Protection Officer has relevant work experience and professional knowledge, and is familiar with laws and administrative regulations related to personal information protection; (2) Whether the Personal Information Protection Officer has clearly defined responsibilities and has been granted sufficient authority to coordinate relevant internal departments and personnel of the personal information processor; (3) Whether the Personal Information Protection Officer has the authority to provide relevant opinions and recommendations prior to the making of decisions on significant matters concerning personal information processing; (4) Whether the Personal Information Protection Officer has the authority to stop non-compliant operations in the personal information processing within the personal information processor and to take necessary corrective measures; (5) Whether the personal information processor has made public the contact information of the Personal Information Protection Officer and has reported the name, contact information, and other details of the Personal Information Protection Officer to the competent authority.	☐Compliant ☐Non-compliant ☐Not Applicable	
22	When conducting a compliance audit on a personal information processor's conduct of personal information protection impact assessments, the following shall be the focus of examination of the conduct and content of the impact assessment: (1) Whether, in accordance with the provisions of laws and administrative regulations, a personal information protection impact assessment has been conducted prior to conducting personal information processing activities that have a significant impact on the rights and interests of individuals; (2) Whether an assessment of the lawfulness, legitimacy, and necessity of the purpose and manner of personal information processing has been conducted; (3) Whether an assessment of the impact on the rights and interests of individuals and the associated security risks has been conducted;	☐Compliant ☐Non-compliant ☐Not Applicable	

	(4) Whether an assessment of the lawfulness and effectiveness of the protective measures adopted, and their appropriateness in relation to the level of risk, has been conducted.		
23	Personal information processors shall formulate emergency response plans for personal information security incidents. During compliance audits, the comprehensiveness, effectiveness, and enforceability of the emergency response plan shall be evaluated, including but not limited to the following: (1) Whether, in combination with actual business conditions, a systematic assessment and forecast of the personal information security risks faced has been conducted; (2) Whether the overall requirements, basic strategies, organizational structure and personnel, technical and material support, command and disposal procedures, emergency and support measures, and other elements are sufficient to address the anticipated risks; (3) Whether relevant personnel have been trained on the emergency response plan, and whether drills are regularly conducted on the emergency response plan.	☐Compliant ☐Non-compliant ☐Not Applicable	
24	When conducting a compliance audit on a personal information processor's emergency response and processing of personal information security incidents, the following items shall be the focus of examination: (1) Whether, in accordance with the emergency response plan and operating procedures, the impact, scope, and potential harm of personal information security incidents have been promptly ascertained, the causes of incidents have been analyzed and identified, and measures to prevent the escalation of harm have been proposed; (2) Whether a notification channel has been established, and whether the competent authority and individuals have been promptly notified in accordance with relevant provisions after a security incident occurs; (3) Whether appropriate measures have been taken to minimize the potential losses and harm risks that may be caused by personal information security incidents.	☐Compliant ☐Non-compliant ☐Not Applicable	

Annex2

Personal Information Protection Impact Assessment Form for Small-Scale Personal Information Processors

No.	Impact Assessment Scenario	Impact Assessment Content	Impact Assessment Conclusion	Remarks
1	Processing sensitive personal information	Whether the purpose, method, and other aspects of personal information processing are lawful, legitimate, and necessary	☐Yes ☐No ☐N/A	
		Impact on the rights and interests of individuals and associated security risks	☐No Impact ☐Has Impact ☐N/A	
		Whether the protective measures adopted are lawful, effective, and appropriate in relation to the level of risk	☐Yes ☐No ☐N/A	
2	Using personal information for automated decision-making	Whether the purpose, method, and other aspects of personal information processing are lawful, legitimate, and necessary	☐Yes ☐No ☐N/A	
		Impact on the rights and interests of individuals and associated security risks	☐No Impact ☐Has Impact ☐N/A	
		Whether the protective measures adopted are lawful, effective, and appropriate in relation to the level of risk	☐Yes ☐No ☐N/A	
3	Entrusting the processing of personal information, providing personal information to other personal information processors, and disclosing personal information	Whether the purpose, method, and other aspects of personal information processing are lawful, legitimate, and necessary	☐Yes ☐No ☐N/A	
		Impact on the rights and interests of individuals and associated security risks	☐No Impact ☐Has Impact ☐N/A	
		Whether the protective measures adopted are lawful, effective, and appropriate in relation to the level of risk	☐Yes ☐No ☐N/A	

4	Providing personal information to overseas recipients	Whether the purpose, method, and other aspects of personal information processing are lawful, legitimate, and necessary	☐Yes ☐No ☐N/A	
		Impact on the rights and interests of individuals and associated security risks	☐No Impact ☐Has Impact ☐N/A	
		Whether the protective measures adopted are lawful, effective, and appropriate in relation to the level of risk	☐Yes ☐No ☐N/A	
5	Other personal information processing activities that have a significant impact on the rights and interests of individuals	Whether the purpose, method, and other aspects of personal information processing are lawful, legitimate, and necessary	☐Yes ☐No ☐N/A	
		Impact on the rights and interests of individuals and associated security risks	☐No Impact ☐Has Impact ☐N/A	
		Whether the protective measures adopted are lawful, effective, and appropriate in relation to the level of risk	☐Yes ☐No ☐N/A	