

Notice of the Cyberspace Administration of China and the Ministry of Public Security on the Provisions on the Protection of Personal Information on Large Online Platforms (Draft for Comments) for Public Comments

November 22, 2025 16:00 Source: [China Cyberspace Network](#)

In order to regulate the personal information processing activities of large online platforms, protect the legitimate rights and interests of personal information, and promote the healthy development of the platform economy, in accordance with the Personal Information Protection Law of the People's Republic of China, the Data Security Law of the People's Republic of China, the Cybersecurity Law of the People's Republic of China, the Regulations on the Management of Network Data Security, and other laws and regulations, the Cyberspace Administration of China and the Ministry of Public Security have drafted the "Provisions on the Protection of Personal Information on Large Online Platforms (Draft for Comments)", which are now open to the public for comments. The public can provide feedback through the following channels and means:

1. Log in to China Cyberspace Administration (www.cac.gov.cn) and enter the homepage "Cyberspace News" to view the manuscript.
2. Log in to the official website of the Ministry of Public Security (www.mps.gov.cn) and enter the homepage "Investigation and Solicitation" to view the manuscript.
3. Send by email to: shujuju@cac.gov.cn.
4. Send comments by letter to: Network Data Administration, Cyberspace Administration of China, No. 15 Fucheng Road, Haidian District, Beijing, zip code 100048, and indicate "Solicitation of Opinions on Personal Information Protection Regulations on Large Online Platforms" on the envelope.

The deadline for feedback is December 22, 2025.

Attachment: Provisions on the Protection of Personal Information on Large Online Platforms (Draft for Comments)

Cyberspace Administration of China Ministry of Public Security

November 22, 2025

Regulations on the protection of personal information on large online platforms

(Draft for Comments)

Article 1: These Provisions are formulated in accordance with the Personal Information Protection Law of the People's Republic of China, the Data Security Law of the People's Republic of China, the Cybersecurity Law of the People's Republic of China, the Regulations on the Management of Network Data, and other laws and regulations, in order to regulate the personal information processing activities of large online platforms, protect the lawful rights and interests of personal information, and promote the rational use of personal information in accordance with law.

Article 2: These Provisions apply to the protection of personal information of large-scale online platforms built and operated within the territory of the People's Republic of China. Where laws and administrative regulations provide otherwise, those provisions shall prevail.

Article 3: The state cyberspace department, in conjunction with the public security department of the State Council and other relevant departments, formulates and publishes a directory of large-scale online platforms and dynamically updates them.

The identification of large network platforms mainly considers the following factors:

- (1) More than 50 million registered users or more than 10 million monthly active users;
- (2) Providing important network services or business scope covering multiple types of business;
- (3) Once the data is leaked, tampered with, or damaged, it will have an important impact on national security, economic operation, and the national economy and people's livelihood;
- (4) Other circumstances provided by the state cyberspace department and the public security department of the State Council.

Article 4: Network data processors providing large-scale online platform services (hereinafter referred to as large-scale online platform service providers) shall follow the principles of lawfulness, legitimacy, necessity, and good faith, abide by laws and regulations, abide by social morality and ethics, assume primary responsibility for the security of the personal information they process, strictly protect sensitive personal information and minors' personal information, and assume social responsibility. The legitimate rights and interests of the organization.

Article 5: Large online platform service providers shall designate a person in charge of personal information protection in accordance with relevant provisions of laws and regulations, and disclose the contact information of the person in charge of

personal information protection.

The person in charge of personal information protection shall be a member of the management of a large online platform service provider, have the nationality of the People's Republic of China, have no permanent residency or long-term residence permit abroad, have professional knowledge of personal information protection, and have been engaged in related work for more than 5 years. The person in charge of personal information protection may also serve as the person in charge of network data security.

The person in charge of personal information protection shall perform the following duties:

(1) Guide large online platforms to carry out personal information processing activities in compliance, implement the personal information protection supervision requirements of the state cyberspace department, the public security department of the State Council, and relevant competent departments, and cooperate with relevant departments to carry out personal information protection supervision and inspection;

(2) Participate in decision-making related to the handling of personal information on large online platforms, and have the right to veto matters handled by personal information;

(3) Responsible for supervising personal information processing activities and protective measures adopted, and if it is found that there are significant security risks or violations of laws and regulations in the personal information processing activities of large online platforms, measures shall be taken immediately and reported to the state cyberspace department and relevant competent departments.

(4) Organize the formulation of special rules for the handling of minors' personal information.

The person in charge of personal information protection may directly report to the state cyberspace department and relevant competent departments on the protection of personal information of large online platform service providers.

Article 6: Large online platform service providers shall specify personal information protection work institutions and carry out personal information protection related work under the leadership of the person in charge of personal information protection, including but not limited to:

(1) Formulate and implement internal personal information protection management systems, operating procedures, and emergency plans for personal information security incidents, reasonably determine the operational authority for personal information processing, and safely manage personal information processing activities on large online platforms;

(2) Organize and carry out activities such as personal information security risk monitoring, risk assessment, compliance audit, impact assessment, emergency drills, publicity, education, and training, and promptly handle personal information security risks and incidents;

(3) Clarify the regulations for the processing of personal information and the obligations of product or service providers on the platform to protect personal information, and supervise their personal information processing activities and performance of personal information protection obligations;

(4) Specify a dedicated person responsible for the protection of minors' personal information;

(5) Accept and handle personal information protection complaints and reports;

(6) Compile and publish a social responsibility report on personal information protection of large online platform service providers every year.

Encourage large online platform service providers to set up special personal information protection agencies.

Article 7: Large online platform service providers shall provide necessary support for those responsible for personal information protection and personal information protection agencies in performing their duties.

Article 8: Large-scale online platform service providers shall promptly submit the following information to the state cyberspace department:

(1) Basic information of the person in charge of personal information protection;

(2) Basic information of the personal information protection work organization;

(3) Measures to ensure that the person in charge of personal information protection and the personal information protection work organization perform their duties.

Where there is a change in the person in charge of personal information protection, personal information protection work organizations, etc., the large online platform service provider shall submit the change information within 20 working days.

The state cyberspace department shall share information on large-scale network platform service providers with the public security department of the State Council and relevant competent departments.

Article 9: Large-scale online platform service providers shall store personal information collected and generated in the course of operations within the territory of the People's Republic of China. If it is really necessary to provide it overseas, it shall comply with the relevant provisions of the national data transfer security management.

Large-scale online platform service providers shall improve technical and management measures related to the security of cross-border personal information transfer in accordance with relevant national regulations, and promptly prevent and deal with security risks and threats of personal information exports that violate laws and regulations.

Article 10: Large-scale online platform service providers shall store personal information collected and generated in the course of operations in the People's Republic of China in data centers that meet the following conditions:

(1) It is established within the territory of the People's Republic of China;

(2) The principal responsible person has the nationality of the People's Republic of China and does not have the right of permanent residence or long-term residence permit abroad;

(3) The safety meets the requirements of relevant national standards.

Article 11: Data centers shall assist large network platform service providers in fulfilling their personal information protection obligations, including but not limited to:

(1) Establish and improve internal personal information management systems and operating procedures;

(2) Where it is discovered that there are security defects, loopholes, or other risks in systems, network products, or services that affect the performance of personal information protection obligations by large online platform service providers, they shall immediately take remedial measures, report to the relevant competent departments in accordance with regulations, and notify the person in charge of personal information protection of the large online platform service provider;

(3) In the event of a personal information security incident, the person in charge of personal information protection of the service provider of a large online platform shall be immediately notified, and emergency response plans shall be promptly activated, measures shall be taken to prevent the spread of harm, and potential security hazards shall be eliminated, and reported to the state cyberspace department and relevant competent departments in accordance with regulations;

(4) Promptly implement the relevant requirements for personal information security protection by the state cyberspace department, the public security department of the State Council, and relevant competent departments.

Article 12: Where a large-scale network platform service provider entrusts a third-party data center that meets the requirements of Article 10 of these Provisions to store personal information, it shall sign a contract with it, agree on the storage location, scale, type, etc., and clearly perform the security requirements of Article 11 of these Provisions and the following duties:

(1) Strictly follow the provisions of laws and regulations and contractual agreements, perform personal information protection obligations, provide safe, stable, and continuous services, and accept the supervision of the person in charge of personal information protection of large online platform service providers, personal information protection supervision committees, etc.;

(2) Provide facilitation measures for large online platform service providers to handle personal information;

(3) Assist large online platform service providers in the security management of personal information processing activities.

Article 13: Large-scale network platform service providers shall submit basic information about data centers that store personal information to the state cyberspace department and other relevant departments, including the management team and management structure, internal personal information protection management systems, security measures adopted, and contract texts signed with third-party data centers. If the above information changes, the change information shall be submitted within 10 working days from the date of change.

Article 14: Large online platform service providers shall provide convenient methods and means for individuals to exercise their rights to access, copy, correct, supplement, delete, or restrict the processing of their personal information, or to cancel their accounts or withdraw consent.

Where individuals request the transfer of their personal information to their designated personal information processors, large online platform service providers shall transfer personal information in a general, machine-readable format within 30 working days after receiving the individual's request, and inform the individual of the processing results by email, telephone, text message, etc. If the processing period needs to be extended due to the number of requests, complex operations, etc., the reason for the extension shall be explained to the individual, and it may be extended by another 30 working days if reasonable and necessary. Where laws, administrative regulations, and departmental rules provide otherwise, those provisions shall prevail.

Support large network platform service providers to provide transfer channels through application programming interfaces or other standardized technical methods, and adopt security measures such as identity verification and encrypted transmission to ensure the security of personal information transfer.

If an individual repeatedly transfers personal information, the large online platform service provider may charge the necessary fees based on the cost of transferring personal information.

Article 15: Large-scale online platform service providers shall carry out personal information protection compliance audits, risk assessments, and other activities on their own or by entrusting third-party professional institutions in accordance with relevant state regulations, and rectify any problems found. Encourage large network platform service providers to give preference to certified third-party professional institutions. The certification of professional institutions shall be carried out in accordance with the relevant provisions of the Regulations of the People's Republic of China on Accreditation and Accreditation.

Article 16: Third-party professional institutions entrusted by large online platform service providers to carry out personal information protection compliance audits, risk assessments, and other activities shall be registered within the territory of the

People's Republic of China, and may report directly to the state cyberspace department and relevant competent departments if they discover that the personal information processing activities of large online platform service providers pose significant security risks or violate laws and regulations; Those suspected of violating the law or committing a crime shall report the case to the public security organs.

Article 17: Where a large online platform service provider has any of the following circumstances, the state cyberspace department, the public security department under the State Council, and relevant competent departments may require it to entrust a third-party professional institution to conduct compliance audits, risk assessments, and other activities for its personal information processing activities:

- (1) Personal information processing activities seriously affect personal rights and interests or seriously lack security measures;
- (2) Repeatedly violating laws and regulations such as illegal departure of personal information;
- (3) Personal information processing activities may infringe on the rights and interests of many individuals;
- (4) Personal information security incidents occur, resulting in the leakage, alteration, loss, or damage of personal information of more than 1 million people or sensitive personal information of more than 100,000 people;
- (5) Other circumstances stipulated by laws and regulations and relevant competent departments.

Large-scale network platform service providers shall cooperate with third-party professional institutions in performing their duties and provide necessary guarantees for third-party professional institutions to carry out their work, including providing necessary access to large-scale network data facilities, systems, and operation log recording rights for designated personnel of third-party professional institutions.

If it is found that large online platform service providers are unable to ensure the security of personal information, the state cyberspace department, the public security department of the State Council, and relevant competent departments may require large online platform service providers to store personal information in third-party data centers that meet the requirements of these Provisions by signing contracts or other means.

Article 18: Encourage large online platform service providers to apply national network identity authentication public services, use data label identification technology, and pass personal information protection certification to improve the level of personal information protection.

Article 19: Encourage large online platform service providers to carry out innovation in personal information protection-related technologies, products, and services, actively participate in the formulation of international standards and rules related to personal information protection, and promote coordination and mutual recognition of personal information protection rules and standards with other countries and regions.

Article 20: Any organization or individual has the right to complain or report to the departments performing personal information protection duties regarding activities that violate these provisions by large network platform service providers and third-party data centers. The department receiving the complaint or report shall handle it in accordance with the law within 15 working days, and inform the complainant or informant of the handling results.

Departments performing personal information protection duties shall strengthen information sharing and coordinate relevant work.

Article 21: Where internet information departments, public security organs, and relevant competent departments discover that large network platform service providers, third-party professional institutions, or data centers have failed to perform their personal information protection responsibilities, they shall be investigated for responsibility in accordance with law; if a crime is constituted, criminal responsibility shall be pursued in accordance with law.

Article 22: Personnel of the State Cyberspace Department, the State Council Public Security Department and relevant competent departments, third-party data centers, and third-party professional institutions shall keep confidential personal privacy, personal information, trade secrets, confidential business information, etc. learned in the course of their work in accordance with law, and must not disclose or illegally provide them to others.

Article 23: The provisions of the Law of the People's Republic of China on the Protection of State Secrets and other laws and administrative regulations shall apply to the handling of personal information involving state secrets and work secrets.

Large network platforms shall implement the relevant requirements for network security level protection, and large network platforms belonging to critical information infrastructure shall also comply with relevant national regulations on the security of critical information infrastructure.

Article 24 These Provisions shall come into force on X year, X, X.