Translation: Personal Information Protection Law of the People's Republic of China (Draft) (Second Review Draft) – April 2021

by:
Graham Webster

Published
April 29, 2021

Last Revision
May 2, 2021

Aug. 20, 2021, update: The final version of the law has been published, and our translation is available here.

This translation of the draft released following the second reading on the Personal Information Protection Law at the National People's Congress Standing Committee was produced based on DigiChina's earlier translation by Rogier Creemers, Mingli Shi, Lauren Dudley, and Graham Webster of the first draft, published Oct. 21, 2020.

[This translation was revised on May 2, 2021; DigiChina thanks Jamie Horsley for valuable comments and corrections.]

Personal Information protection Law of the People's Republic of China (Draft) (Second Review Draft)

Table of Contents

Chapter I: General Provisions

Article 1: This Law is formulated in order to protect personal information rights and interests, standardize personal information handling activities, and promote the rational use of personal information.

Article 2: The personal information of natural persons receives legal protection; no organization or individual may infringe natural persons' personal information rights and interests.

Article 3: This Law applies to organizations and individuals' handling personal information activities of natural persons within the borders of the People's Republic of China.

Where one of the following circumstances is present in handling activities outside the borders of the People's Republic of China of personal information of natural persons within the borders of the People's Republic of China, this Law applies as well:

1. Where the purpose is to provide products or services to natural persons inside the borders;

2. Where analyzing or assessing activities of natural persons inside the borders;

3. Other circumstances provided in laws or administrative regulations.

Article 4: Personal information is all kinds of information recorded by electronic or other means related to identified or identifiable natural persons, not including information after anonymization handling.

Personal information handling includes personal information collection, storage, use, processing, transmission, provision, publishing, etc.

Article 5: Lawful and proper methods shall be adopted for personal information handling, and the principle of sincerity observed. It is prohibited to handle personal information in misleading, swindling, coercive, or other such ways.

Article 6: Personal information handling shall have a clear and reasonable purpose, and shall be limited to the smallest scope and a method with the smallest influence on individual rights and interests necessary to realize the handling purpose. It is prohibited to conduct personal information handling unrelated to the handling purpose.

Article 7: The principles of openness and transparency shall be observed in the handling of personal information, disclosing the rules for handling personal information and clearly indicating the purpose, method, and scope of handling.

Article 8: The handling of personal information shall ensure the quality of personal information, and avoid adverse effects on individual rights and interests from inaccurate or incomplete personal information

Article 9: Personal information handlers shall bear responsibility for their personal information handling activities, and adopt the necessary measures to safeguard the security of the personal information they handle.

Article 10: No organization or individual may handle personal information in violation of the provisions of laws and administrative regulations, or engage in personal information handling activities harming national security or the public interest.

Article 11: The State establishes a personal information protection structure, to prevent and punish acts harming personal information rights and interests, strengthen personal information protection propaganda and education, and promote the creation of a good environment for personal information protection, with joint participation from government, enterprise, relevant sectoral organizations, and the general public.

Article 12: The State vigorously participates in the formulation of international rules [or norms] for personal information protection, stimulates international exchange and cooperation in the area of personal information protection, and promotes mutual recognition of personal information protection rules [or norms], standards, etc., with other countries, regions, and international organizations.

Chapter II: Personal Information Handling Rules

Section 1: Common Provisions

Article 13: Personal information handlers may only handle personal information where they conform to one of the following circumstances:

1. Obtaining individuals' consent;

2. Where necessary to conclude or fulfill a contract in which the individual is an interested party;

3. Where necessary to fulfill statutory duties and responsibilities or statutory obligations;

4. Where necessary to respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property, under emergency conditions;

5. When handling previously disclosed personal data within a reasonable scope in accordance with the provisions of this Law.

6. Handling personal information within a reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest;

7. Other circumstances provided in laws and administrative regulations.

In accordance with other relevant provisions of this Law, when handling of personal information, individual consent shall be obtained. However, obtaining individual consent is not required under conditions in items 2 through 7 above.

Article 14: Consent for handling personal information shall be given by individuals under the precondition of full knowledge, and in a voluntary and explicit statement. Where laws or administrative regulations provide that separate consent or written consent shall be obtained to handle personal information, those provisions are followed.

Where a change occurs in the purpose of personal information handling, the handling method, or the categories of handled personal information, the individual's consent shall be obtained again.

Article 15: Where personal information handlers handle the personal information of a minor under the age of 14, they shall obtain the consent of the minor's parents or other guardians.

Article 16: Individuals have the right to rescind their consent to personal information handling activities conducted on the basis of individuals' consent. Personal information handlers shall provide a convenient way to withdraw consent.

If an individual rescinds consent, it does not affect the effectiveness of personal information handling activities undertaken on the basis of individual consent before consent was rescinded.

Article 17: Personal information handlers may not refuse to provide products or services on the basis that an individual does not consent to the handling of their personal information or rescinds their consent to handle personal information, except where handling personal information is necessary for the provision of products or services.

Article 18: Personal information handlers shall, before handling personal information, explicitly notify individuals of the following items using clear and easily understood language:

1. The identity and contact method of the personal information handler;

2. The purpose of personal information handling and handling methods, the categories of handled personal information, and retention period;

3. Methods and procedures for individuals to exercise the rights provided in this Law;

4. Other items that laws or administrative regulations provide shall be notified.

Where a change occurs in the matters provided in the previous paragraph, individuals shall be notified about the change.

Where personal information handlers notify the matters as provided in Paragraph I through the method of formulating personal information handling rules, the handling rules shall be public and convenient to read and store.

Article 19: Personal information handlers handling personal information are permitted not to notify individuals about the items provided in the previous Article under circumstances where laws or administrative regulations provide that secrecy shall be preserved or notification is not necessary

Under emergency circumstances, where it is impossible to notify individuals in a timely manner in order to protect natural persons' lives, health, and the security of their property, personal information handlers shall notify them after the conclusion of the emergency circumstances.

Article 20: Personal information retention periods shall be the shortest period necessary to realize the purpose of the personal information handling. Where laws or administrative regulations provide otherwise concerning personal information retention periods, those provisions are followed.

Article 21: Where two or more personal information handlers jointly decide on a personal information handling purpose and handling method, they shall agree on the rights and obligations of each. However, said agreement does not influence an individual's rights to demand any one personal information handler perform under this Law's provisions.

Where personal information handlers jointly handling personal information harm personal information rights and interests, they bear joint liability according to the law.

Article 22: Where personal information handlers entrust the handling of personal information, they shall conclude an agreement with the entrusted party on the purpose for entrusted handling, the time limit, the handling method, categories of personal information, protection measures, as well as the rights and duties of both sides, etc., and conduct supervision of the personal information handling activities of the entrusted party.

Entrusted parties shall handle personal information according to the agreement; they may not handle personal information for handling purposes or in handling methods, etc., in excess of the agreement. If the entrusting contract does not take effect, is void, has been cancelled, or has been terminated, the entrusted party shall return the personal information to the personal information handler or delete it and may not retain it.

Without the consent of the personal information handler, an entrusted party may not further entrust personal information handling to other persons.

Article 23: Personal information handlers shall, where it is necessary to transfer personal information due to mergers, separations, and other such reasons, notify individuals about the receiving party's identity and contact method. The receiving party shall continue to fulfill the personal information handler's duties. Where the receiving side changes the original handling purpose or handling method, they shall notify the individual again as provided in this Law.

Article 24: Where personal information handlers provide others with the personal information they handle, they shall notify individuals about the identity of the recipient, their contact method, the handling purpose, handling method, and personal information categories, and obtain the separate consent from the individual. Recipients shall handle personal information within the above mentioned scope of handling purposes, handling methods, personal information categories, etc. Where recipients change the original handling purpose or handling methods, they shall again obtain the individual's consent.

Article 25: When using personal information to conduct automated decision making, the transparency of the decision making and the fairness and reasonableness of the handling result shall be guaranteed.

Those conducting commercial sales or information push delivery through automated decision making methods, shall simultaneously provide the option to not target an individual's characteristics, or provide the individual with a method to refuse.

When the use of automated decision-making produces decisions with a major influence on the rights and interests of the individual, they have the right to require personal information handlers to explain the matter, and they have the right to refuse that personal information handlers make decisions solely through automated decision making methods.

Article 26: Personal information handlers may not publish the personal information they handle; except where they obtain separate consent.

Article 27: The installation of image collection or personal identity recognition equipment in public venues shall occur as required to safeguard public security and observe relevant State regulations, and clear indicating signs shall be installed. Collected personal images and personal identity characteristic information can only be used for the purpose of safeguarding public security; it may not be published or provided to other persons, except where individuals' separate consent is obtained.

Article 28: Personal information handlers handling already disclosed personal information shall respect the purpose for which the personal information was disclosed. If exceeding rational scope related to that purpose, they shall obtain individual consent according to the provisions of this Law.

Where the purpose at the time the personal information was published is not clear, personal information handlers shall handle published personal information in a reasonable and cautious manner; for activities using published personal information having a major influence on individuals, they shall obtain individual consent in accordance with the provisions of this Law.

Section II: Rules for Handling Sensitive Personal Information

Article 29: Personal information handlers may handle sensitive personal information only for specific purposes and when sufficiently necessary.

Sensitive personal information means personal information that, once leaked or illegally used, may cause discrimination against individuals or grave harm to personal or property security,

including information on race, ethnicity, religious beliefs, individual biometric features, medical health, financial accounts, individual location tracking, etc.

Article 30: Where handling sensitive personal information based on individual consent, personal information handlers shall obtain separate consent from the individual. Where laws or administrative regulations provide that written consent is obtained for handling sensitive personal information, those provisions are followed.

Article 31: Personal information handlers handling sensitive personal information, in addition to the items set out in Article 18 Item 1 of this Law, shall also notify individuals of the necessity and effects on the individual of handling the sensitive personal information.

Article 32: Where laws or administrative regulations provide that relevant administrative licenses shall be obtained or other restrictions apply to the handling of sensitive personal information, those provisions are followed.

Section III: Specific Provisions on State Organs Handling Personal Information

Article 33: This Law applies to State organs' activities of handling personal information; where this Section contains specific provisions, the provisions of this Section apply.

Article 34: State organs handling personal information to fulfill their statutory duties and responsibilities shall conduct them according to the powers and procedures provided in laws or administrative regulations; they may not exceed the scope or extent necessary to fulfill their statutory duties and responsibilities.

Article 35: State organs handling personal information for the purpose of fulfilling statutory duties and responsibilities shall notify individuals according to the provisions of this Law and obtain their consent, except where laws or administrative regulations provide that secrecy shall be protected, or where notification and obtaining consent will impede State organs' fulfillment of their statutory duties and responsibilities.

Article 36: Personal information handled by State organs shall be stored within the mainland territory of the People's Republic of China. If it is necessary to provide it abroad, a risk assessment shall be undertaken. Relevant authorities may be requested to support and assist with risk assessment.

Article 37: The provisions of this Law regarding personal information handling by State organs apply to organizations handling personal information in order to fulfill their duties while performing functions related to managing public affairs as authorized by laws and administrative regulations.

Chapter III: Rules on the Cross-Border Provision of Personal Information

Article 38: Where personal information handlers need to provide personal information outside the borders of the People's Republic of China for business or other such requirements, they shall meet at least one of the following conditions:

1. Passing a security assessment organized by the State cybersecurity and informatization department according to Article 40 of this Law;

2. Undergoing personal information protection certification conducted by a specialized body according to provisions by the State cybersecurity and informatization department;

3. Concluding a contract with the foreign receiving side in accordance with a standard contract formulated by the cyberspace and informatization department, agreeing upon the rights and responsibilities of both sides, and supervising such that personal information handling activities satisfy the standard of personal information protection provided for in this Law.

4. Other conditions provided in laws or administrative regulations or by the State cybersecurity and informatization department.

Article 39: Where personal information handlers provide personal information outside of the borders of the People's Republic of China, they shall notify the individual about the foreign receiving side's identity, contact method, handling purpose, handling methods, and personal information categories, as well as ways for individuals to exercise the rights provided in this Law with the foreign receiving side, and other such matters, and obtain individuals' separate consent.

Article 40: Critical information infrastructure operators and personal information handlers handling personal information reaching quantities provided by the State cybersecurity and informatization department shall store personal information collected and produced within the borders of the People's Republic of China domestically. Where they need to provide it abroad,

they shall pass a security assessment organized by the State cybersecurity and informatization department; where laws or administrative regulations and State cybersecurity and informatization department provisions permit that security assessment not be conducted, those provisions are followed.

Article 41: When a judicial or law enforcement organization from outside the mainland territory of the People's Republic of China requests the provision of personal information stored within the territory, it shall not be provided without the approval of the organ in charge. Where an international treaty or agreement concluded or participated in by the People's Republic of China provides, those provisions may be carried out.

Article 42: Where foreign organizations or individuals engage in personal information handling acts harming personal information rights and interests of citizens of the People's Republic of China, or harming the national security or public interest of the People's Republic of China, the State cybersecurity and informatization department may put them on a list limiting or prohibiting personal information provision, issue a warning, and adopt measures such as limiting or prohibiting the provision of personal information to them, etc.

Article 43: Where any country or region adopts discriminatory prohibitions, limitations or other similar measures against the People's Republic of China in the area of personal information protection, the People's Republic of China may adopt retaliatory measures against said country or region on the basis of actual circumstances.

Chapter IV: Individuals' Rights in Personal Information Handling Activities

Article 44: Individuals have the right to know and the right to decide relating to their personal information, and have the right to limit or refuse the handling of their personal information by others, unless laws or administrative regulations stipulate otherwise.

Article 45: Individuals have the right to access and copy their personal information from personal information handlers, except in circumstances provided in Article 19 Paragraph I of this Law.

Where individuals request to access or copy their personal information, personal information handlers shall provide it in a timely manner.

Article 46: Where individuals discover their personal information is incorrect or incomplete, they have the right to request personal information handlers correct or complete their personal information. Where individuals request to correct or complete their personal information, personal information handlers shall verify the personal information and correct or complete it in a timely manner.

Where individuals request to correct or complete their personal information, personal information handlers shall verify the personal information and correct or complete it in a timely manner.

Article 47: Personal information handlers shall actively delete personal information where one of the following circumstances occurs; if the personal information handler has not deleted, individuals have the right to request deletion:

1. The handling purpose has been achieved or [the personal information] is no longer necessary to achieve the handling purpose;

2. Personal information handlers cease the provision of products or services, or the retention period has expired;

3. The individual rescinds consent;

4. Personal information handlers handled personal information in violation of laws, administrative regulations, or agreements;

5. Other circumstances provided by laws or administrative regulations.

Where the retention period provided by laws or administrative regulations has not expired, or personal information deletion is technically hard to realize, personal information handlers shall cease personal information handling except for storage and taking necessary security protective measures.

Article 48: Individuals have the right to request personal information handlers explain personal information handling rules.

Article 49: When a natural person is deceased, the rights of the individual as to personal information handling activities according to the provisions of this Chapter shall be exercised by

the next of kin.

Article 50: Personal information handlers shall establish mechanisms to accept and handle applications from individuals to exercise their rights. Where they reject individuals' requests to exercise their rights, they shall explain the reason.

Chapter V: Personal Information Handlers' Duties

Article 51: Personal information handlers shall, on the basis of the personal information handling purpose, handling methods, personal information categories, as well as the influence on individuals, possibly existing security risks, etc., adopt the necessary measures to ensure personal information handling conforms to the provisions of laws and administrative regulations, and prevent unauthorized access as well as personal information leaks or theft, distortion, or deletion:

1. Formulating internal management structures and operating rules;

2. Implementing categorized management of personal information;

3. Adopting corresponding technical security measures such as encryption, de-identification, etc.;

4. Reasonably determining operational limits for personal information handling, and regularly conducting security education and training for employees;

5. Formulating and organizing the implementation of personal information security incident response plans;

6. Other measures provided in laws or administrative regulations.

Article 52: Personal information handlers who handle personal information reaching quantities provided by the State cybersecurity and informatization department shall appoint persons responsible for personal information protection, responsible for conducting supervision of personal information handling activities as well as adopted protection measures, etc.

Personal information handlers shall disclose the methods of contacting persons responsible for personal information protection, and report the names of the responsible persons and contact

methods to the departments fulfilling personal information protection duties and responsibilities.

Article 53: Personal information handlers outside the borders of the People's Republic of China as provided in Article 3 Paragraph II of this Law shall establish a dedicated entity or appoint a representative within the borders of the People's Republic of China, to be responsible for matters related to the personal information they handle, and will report the name of the relevant entity or the name and contact method, etc., of the representative to the departments fulfilling personal information protection duties and responsibilities.

Article 54: Personal information handlers shall regularly engage in audits of their personal information handling activities and compliance with laws and administrative regulations.

Article 55: Personal information handlers shall conduct a risk assessment in advance of the following personal information handling activities, and record the handling situation:

1. Handling sensitive personal information;

2. Using personal information to conduct automated decision making;

3. Entrusting personal information handling, providing personal information to others, or disclosing personal information;

4. Providing personal information abroad;

5. Other personal information handling activities with a major influence on individuals.

The risk assessment content shall include:

1. Whether or not the personal information handling purpose, handling method, etc., are lawful, legitimate, and necessary;

2. The influence on individuals and the degree of risk;

3. Whether security protection measures undertaken are legal, effective, and suitable to the degree of risk.

Risk assessment reports and handling status records shall be preserved for at least three years.

Article 56: Where personal information handlers discover a personal information leak, they shall immediately adopt remedial measures, and notify the departments fulfilling personal information protection duties and responsibilities and the individuals. The notification shall include the following items:

1. The cause of the personal information leak;

2. The categories of leaked personal information and the harm that may be created;

3. Adopted remedial measures;

4. Measures individuals may adopt to mitigate harm;

5. Contact method of the personal information handler.

Where personal information handlers adopt measures that are able to effectively avoid harm created by information leaks, personal information handlers are permitted to not notify individuals; however, where departments fulfilling personal information protection protection duties and responsibilities believe a personal information leak may create harm to individuals, they may require personal information handlers to notify individuals.

Article 57: Personal information handlers providing basic Internet platform services, who have a large number of users, and whose business models are complex shall fulfill the following obligations:

1. Establish an independent body composed mainly of outside members to supervise personal information handling activities;

2. Stop providing services to products or service providers on the platform that seriously violate laws or administrative regulations in handling personal information;

3. Regularly release personal information protection social responsibility reports, and accept society's supervision.

Article 58: Entrusted parties accepting entrusted handling of personal information shall perform the relevant duties provided by this Chapter, and take necessary measures to safeguard the security of the personal information they handle.

Chapter VI: Departments Fulfilling Personal Information Protection Duties and Responsibilities.

Article 59: The State cybersecurity and informatization department is responsible for comprehensive planning and coordination of personal information protection work and related supervision and management work. Relevant State Council departments are responsible for personal information protection, supervision, and management work within their respective scope of duties and responsibilities, according to the provisions of this Law and relevant laws and administrative regulations.

County-level and higher People's Governments' relevant departments' personal information protection, supervision and management duties and responsibilities are determined according to relevant State regulations.

Departments provided in the previous two Paragraphs are jointly named departments fulfilling personal information protection duties and responsibilities.

Article 60: Departments fulfilling personal information protection duties and responsibilities fulfill the following personal information protection duties and responsibilities:

1. Conducting personal information protection propaganda and education, and guiding and supervising personal information handlers' conduct of personal information protection work;

2. Accepting and handling personal information protection-related complaints and reports;

3. Investigating and handling unlawful personal information handling activities;

4. Other duties and responsibilities provided in laws or administrative regulations.

Article 61: The State cybersecurity and informatization department coordinates overall the following personal information protection work by the relevant departments:

1. Formulate concrete personal information protection rules and standards;

2. Formulate specialized personal information protection rules and standards for new technologies and new applications regarding sensitive personal information, facial recognition, artificial intelligence, etc.;

3. Support the research and development of secure and convenient electronic identity authentication technology;

4. Advance the construction of service systems to socialize personal information protection, and support relevant organizations to launch personal information protection evaluation and certification services.

Article 62: When departments fulfilling personal information protection duties and responsibilities fulfill personal information protection duties and responsibilities, they may adopt the following measures:

1. Interviewing relevant concerned parties, investigating circumstances related to personal information handling activities;

2. Consulting and reproducing a concerned party's contracts, records, receipts as well as other relevant material related to personal information handling activities;

3. Conducting on-side inspections, conducting investigations of suspected unlawful personal information handling activities;

4. Inspecting equipment and articles relevant to personal information handling activities; and when there is evidence the equipment or articles engage in illegal personal information handling activities, after reporting to their department's main responsible person in writing and receiving approval, they may seal or confiscate it.

Where departments fulfilling personal information protection duties and responsibilities fulfill their duties and responsibilities according to the law, concerned parties shall provide assistance and cooperation, and they may not obstruct or impede them.

Article 63: Where departments fulfilling personal information protection duties and responsibilities discover relatively large risks exist in personal information handling activities or

personal information security incidents occur, they may conduct a talk with the personal information handler's legal representative or main responsible person according to regulatory powers and procedures, or require personal information handlers to entrust specialized institutions to conduct compliance audits of their personal information handling activities. Personal information handlers shall adopt measures according to requirements to correct the matter and eliminate the vulnerability.

Article 64: Any organization or individual has the right to file a complaint or report about unlawful personal information handling activities with departments fulfilling personal information protection duties and responsibilities. Departments receiving complaints or reports shall handle them promptly and according to the law, and notify the complaining or reporting person of the handling outcome.

Departments fulfilling personal information protection duties and responsibilities shall publish contact methods to accept complaints and reports.

Chapter VII: Legal Liability

Article 65: Where personal information is handled in violation of this Law or personal information is handled without adopting necessary security protection measures in accordance with regulations, the departments fulfilling personal information protection duties and responsibilities orders correction and confiscate unlawful income; where correction is refused, a fine of not more than 1 million Yuan is additionally imposed; the directly responsible person in charge and other directly responsible personnel are fined between 10,000 and 100,000 Yuan.

Where the circumstances of the unlawful acts mentioned in the preceding Paragraph are grave, the departments fulfilling personal information protection duties and responsibilities order correction, confiscate unlawful income, and impose a fine of not more than 50 million Yuan, or 5% of annual revenue. They may also order the suspension of related business activities, cessation of business for rectification, and report to the relevant competent department for cancellation of corresponding professional licenses or cancellation of business permits. The directly responsible person in charge and other directly responsible personnel are fined between 100,000 and 1 million Yuan.

Article 66: Where unlawful acts as provided in this law occur, they will be entered into credit files as provided by relevant laws and administrative regulations, and be published.

Article 67: Where State organs fail to fulfill the personal information protection duties as provided in this Law, their superior organs or the departments fulfilling personal information protection duties and responsibilities shall order correction; the directly responsible person in charge and other directly responsible persons will be disciplined according to the law.

Article 68: When personal information rights and interests are infringed due to personal information handling activites, and personal information handlers cannot prove they are not at fault, they shall take responsibility for the infringement through compensation, etc.

In the above clause, the responsibility to compensate for infringement shall be determined according to the resulting loss to the individual or the personal information handler's resulting gains. Where the loss to the individual and the personal information handler's profits are difficult to determine, determine compensation according to practical conditions.

Article 69: Where personal information handlers handle personal information in violation of the provisions of this Law, infringing on the rights and benefits of many individuals, the People's Procuratorates, departments fulfilling personal information protection duties and responsibilities, and the State cybersecurity and informatization department may file a lawsuit with a People's Court according to the law.

Article 70: Where a violation of the provisions of this Law constitutes a violation of public security management, public security management punishment shall be imposed according to the law; where it constitutes a crime, criminal liability is investigated according to the law.

Chapter VIII: Supplemental Provisions

Article 71: This law does not apply to natural persons handling personal information for personal or family affairs.

Where law contains provisions on personal information handling by People's Governments at all levels and relevant departments and organizations implementing statistical and archival management activities, those provisions apply.

Article 72: The following terms of this Law are defined as follows:

1. "Personal information handler" refers to organizations and individuals that autonomously determine handling purposes, handling methods, and other such personal information handling

matters.

2. "Automated decision making" refers to activities that use personal information to automatically analyze, assess, and decide, via computer programs, individual behaviors and habits, interests and hobbies, or situations relating to finance, health, or credit status.

3. "De-identification" refers to the process of personal information undergoing handling to ensure it is impossible to identify specific natural persons without support of additional information.

4. "Anonymization" refers to the process of personal information undergoing handling to make it impossible to distinguish specific natural persons and impossible to restore.

Article 73: This Law shall enter into force on [day, month, year].

Original Chinese-language text

Source: http://www.npc.gov.cn/flcaw/userIndex.html?lid=ff80818178f9100801791b35d78b4eb4

中华人民共和国个人信息保护法(草案)(二次审议稿)

目录

第一章总则

第一条为了保护个人信息权益,规范个人信息处理活动,促进个人信息合理利用,制定本法。

第二条自然人的个人信息受法律保护,任何组织、个人不得侵害自然人的个人信息权益。

第三条组织、个人在中华人民共和国境内处理自然人个人信息的活动,适用本法。

在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动,有下列情形之一的,也适用本法:

(一)以向境内自然人提供产品或者服务为目的;

(二)分析、评估境内自然人的行为;

(三)法律、行政法规规定的其他情形。

第四条个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息,不包括匿名化处理后的信息。

个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等。

第五条处理个人信息应当采用合法、正当的方式,遵循诚信原则,不得通过误导、欺诈、胁迫等方式处理个人信息。

第六条处理个人信息应当具有明确、合理的目的,并应当限于实现处理目的所必要的最小范围、采取对个人权益影响最小的方式,不得进行与处理目的无关的个人信息处理。

第七条处理个人信息应当遵循公开、透明的原则,公开个人信息处理规则,明示处理的目的、方式和范围。

第八条处理个人信息应当保证个人信息的质量,避免因个人信息不准确、不完整对个人权益造成不利影响。

第九条个人信息处理者应当对其个人信息处理活动负责,并采取必要措施保障所处理的个人信息的安全。

第十条任何组织、个人不得违反法律、行政法规的规定处理个人信息,不得从事危害国家安全、公共利益的个人信息处理活动。

第十一条国家建立健全个人信息保护制度,预防和惩治侵害个人信息权益的行为,加强个人信息保护宣传教育,推动形成政府、企业、相关行业组织、社会公众共同参与个人信息保护的良好环境。

第十二条国家积极参与个人信息保护国际规则的制定,促进个人信息保护方面的国际交流与合作,推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等的互认。

第二章 个人信息处理规则

第一节 一般规定

第十三条符合下列情形之一的,个人信息处理者方可处理个人信息:

(一)取得个人的同意;

(二)为订立或者履行个人作为一方当事人的合同所必需;

(三)为履行法定职责或者法定义务所必需;

(四)为应对突发公共卫生事件,或者紧急情况下为保护自然人的生命健康和财产安全所必需;

(五)依照本法规定在合理的范围内处理已公开的个人信息;

(六)为公共利益实施新闻报道、舆论监督等行为,在合理的范围内处理个人信息;

(七)法律、行政法规规定的其他情形。

依照本法其他有关规定,处理个人信息应当取得个人同意,但有前款第二项至第七项规定情形的,不需取得个人同意。

第十四条处理个人信息的同意,应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的,从其规定。

个人信息的处理目的、处理方式和处理的个人信息种类发生变更的,应当重新取得个人同意。

第十五条个人信息处理者处理不满十四周岁未成年人个人信息的,应当取得未成年人的父母或者其他监护人的同意。

第十六条基于个人同意而进行的个人信息处理活动,个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。个人撤回同意,不影响撤回前基于个人同意已进行的个人信息处理活动的效力。

第十七条个人信息处理者不得以个人不同意处理其个人信息或者撤回其对个人信息处理的同意为由,拒绝提供产品或者服务;处理个人信息属于提供产品或者服务所必需的除外。

第十八条个人信息处理者在处理个人信息前,应当以显著方式、清晰易懂的语言向个人告知下列事项:

(一)个人信息处理者的身份和联系方式;

(二)个人信息的处理目的、处理方式,处理的个人信息种类、保存期限;

(三)个人行使本法规定权利的方式和程序;

(四)法律、行政法规规定应当告知的其他事项。前款规定事项发生变更的,应当将变更部分告知个人。个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的,处理规则应当公开,并且便于查阅和保存。

第十九条个人信息处理者处理个人信息,有法律、行政法规规定应当保密或者不需要告知的情形的,可以不向个人告知前条规定的事项。紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的,个人信息处理者应当在紧急情况消除后及时告知。

第二十条个人信息的保存期限应当为实现处理目的所必要的最短时间。法律、行政法规对个人信息的保存期限另有规定的,从其规定。

第二十一条两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的,应当约定各自的权利和义务。但是,该约定不影响个人向其中任何一个个人信息处理者要求行使本法规定的权利。个人信息处理者共同处理个人信息,侵害个人信息权益的,应当承担连带责任。

第二十二条个人信息处理者委托处理个人信息的,应当与受托方约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等,并对受托方的个人信息处理活动进行监督。

受托方应当按照约定处理个人信息,不得超出约定的处理目的、处理方式等处理个人信息;委托合同不生效、无效、被撤销或者终止的,受托方应当将个人信息返还个人信息处理者或者予以删除,不得保留。

未经个人信息处理者同意,受托方不得转委托他人处理个人信息。

第二十三条个人信息处理者因合并、分立等原因需要转移个人信息的,应当向个人告知接收方的身份、联系方式。接收方应当继续履行个人信息处理者的义务。接收方变更原先的处理目的、处理方式,应当依照本法规定重新取得个人同意。

第二十四条个人信息处理者向他人提供其处理的个人信息的,应当向个人告知接收方的身份、联系方式、处理目的、处理方式和个人信息的种类,并取得个人的单独同意。接收方应当在上述处理目的、处理方式和个人信息的种类等范围内处理个人信息。接收方变更原先的处理目的、处理方式的,应当依照本法规定重新取得个人同意。

第二十五条利用个人信息进行自动化决策,应当保证决策的透明度和结果公平合理。通过自动化决策方式进行商业营销、信息推送,应当同时提供不针对其个人特征的选项,或者向个人提供拒绝的方式。通过自动化决策方式作出对个人权益有重大影响的决定,个人有权要求个人信息处理者予以说明,并有权拒绝个人信息处理者仅通过自动化决策的方式作出决定。

第二十六条个人信息处理者不得公开其处理的个人信息,取得个人单独同意的除外。

第二十七条在公共场所安装图像采集、个人身份识别设备,应当为维护公共安全所必需,遵守国家有关规定,并设置显著的提示标识。所收集的个人图像、个人身份特征信息只能用于维护公共安全的目的,不得公开或者向他人提供,取得个人单独同意的除外。

第二十八条个人信息处理者处理已公开的个人信息,应当符合该个人信息被公开时的用途。超出与该用途相关的合理范围的,应当依照本法规定取得个人同意。个人信息被公开时的用途不明确的,个

人信息处理者应当合理、谨慎地处理已公开的个人信息。利用已公开的个人信息从事对个人有重大影响的活动,应当依照本法规定取得个人同意。

第二节 敏感个人信息的处理规则

第二十九条个人信息处理者具有特定的目的和充分的必要性,方可处理敏感个人信息。

敏感个人信息是一旦泄露或者非法使用,可能导致个人受到歧视或者人身、财产安全受到严重危害的个人信息,包括种族、民族、宗教信仰、个人生物特征、医疗健康、金融账户、个人行踪等信息。

第三十条基于个人同意处理敏感个人信息的,个人信息处理者应当取得个人的单独同意。法律、行政法规规定处理敏感个人信息应当取得书面同意的,从其规定。

第三十一条个人信息处理者处理敏感个人信息的,除本法第十八条第一款规定的事项外,还应当向个人告知处理敏感个人信息的必要性以及对个人的影响。

第三十二条法律、行政法规对处理敏感个人信息规定应当取得相关行政许可或者作出其他限制的,从其规定。

第三节国家机关处理个人信息的特别规定

第三十三条国家机关处理个人信息的活动,适用本法;本节有特别规定的,适用本节规定。

第三十四条国家机关为履行法定职责处理个人信息,应当依照法律、行政法规规定的权限、程序进行,不得超出履行法定职责所必需的范围和限度。

第三十五条国家机关为履行法定职责处理个人信息,应当依照本法规定向个人告知并取得其同意;法律、行政法规规定应当保密,或者告知、取得同意将妨碍国家机关履行法定职责的除外。

第三十六条国家机关处理的个人信息应当在中华人民共和国境内存储;确需向境外提供的,应当进行风险评估。风险评估可以要求有关部门提供支持与协助。

第三十七条法律、法规授权的具有管理公共事务职能的组织为履行法定职责处理个人信息,适用本法关于国家机关处理个人信息的规定。

第三章 个人信息跨境提供的规则

第三十八条个人信息处理者因业务等需要,确需向中华人民共和国境外提供个人信息的,应当至少具备下列一项条件:

(一)依照本法第四十条的规定通过国家网信部门组织的安全评估;

(二)按照国家网信部门的规定经专业机构进行个人信息保护认证;

(三)按照国家网信部门制定的标准合同与境外接收方订立合同,约定双方的权利和义务,并监督其个人信息处理活动达到本法规定的个人信息保护标准;

(四)法律、行政法规或者国家网信部门规定的其他条件。

第三十九条个人信息处理者向中华人民共和国境外提供个人信息的,应当向个人告知境外接收方的身份、联系方式、处理目的、处理方式、个人信息的种类以及个人向境外接收方行使本法规定权利的方式等事项,并取得个人的单独同意。

第四十条关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者,应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的,应当通过国家网信部门组织的安全评估;法律、行政法规和国家网信部门规定可以不进行安全评估的,从其规定。

第四十一条中华人民共和国境外的司法或者执法机构要求提供存储于中华人民共和国境内的个人信息的,非经中华人民共和国主管机关批准,不得提供;中华人民共和国缔结或者参加的国际条约、协定有规定的,可以按照其规定执行。

第四十二条境外的组织、个人从事损害中华人民共和国公民的个人信息权益,或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的,国家网信部门可以将其列入限制或者禁止个人信息提供清单,予以公告,并采取限制或者禁止向其提供个人信息等措施。

第四十三条任何国家和地区在个人信息保护方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的,中华人民共和国可以根据实际情况对该国家或者该地区对等采取措施。

第四章 个人在个人信息处理活动中的权利

第四十四条个人对其个人信息的处理享有知情权、决定权,有权限制或者拒绝他人对其个人信息进行处理;法律、行政法规另有规定的除外。

第四十五条个人有权向个人信息处理者查阅、复制其个人信息;有本法第十九条第一款规定情形的除外。

个人请求查阅、复制其个人信息的,个人信息处理者应当及时提供。

第四十六条个人发现其个人信息不准确或者不完整的,有权请求个人信息处理者更正、补充。

个人请求更正、补充其个人信息的,个人信息处理者应当对其个人信息予以核实,并及时更正、补充。

第四十七条有下列情形之一的,个人信息处理者应当主动删除个人信息;个人信息处理者未删除的,个人有权请求删除:

(一)处理目的已实现或者为实现处理目的不再必要;

(二)个人信息处理者停止提供产品或者服务,或者保存期限已届满;

(三)个人撤回同意;

(四)个人信息处理者违反法律、行政法规或者违反约定处理个人信息;

(五)法律、行政法规规定的其他情形。

法律、行政法规规定的保存期限未届满,或者删除个人信息从技术上难以实现的,个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。

第四十八条个人有权要求个人信息处理者对其个人信息处理规则进行解释说明。

第四十九条自然人死亡的,本章规定的个人在个人信息处理活动中的权利,由其近亲属行使。

第五十条个人信息处理者应当建立个人行使权利的申请受理和处理机制。拒绝个人行使权利的请求的,应当说明理由。

第五章 个人信息处理者的义务

第五十一条个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人的影响、可能存在的安全风险等,采取必要措施确保个人信息处理活动符合法律、行政法规的规定,

并防止未经授权的访问以及个人信息泄露或者被窃取、篡改、删除:

(一)制定内部管理制度和操作规程;

(二)对个人信息实行分类管理;

(三)采取相应的加密、去标识化等安全技术措施;

(四)合理确定个人信息处理的操作权限,并定期对从业人员进行安全教育和培训;

(五)制定并组织实施个人信息安全事件应急预案;

(六)法律、行政法规规定的其他措施。

第五十二条处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人,负责对个人信息处理活动以及采取的保护措施等进行监督。个人信息处理者应当公开个人信息保护负责人的联系方式,并将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责的部门。

第五十三条本法第三条第二款规定的中华人民共和国境外的个人信息处理者,应当在中华人民共和国境内设立专门机构或者指定代表,负责处理个人信息保护相关事务,并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。

第五十四条个人信息处理者应当定期对其个人信息处理活动遵守法律、行政法规的情况进行合规审计。

第五十五条个人信息处理者应当对下列个人信息处理活动在事前进行风险评估,并对处理情况进行记录:

(一)处理敏感个人信息;

(二)利用个人信息进行自动化决策;

(三)委托处理个人信息、向他人提供个人信息、公开个人信息;

(四)向境外提供个人信息;

(五)其他对个人有重大影响的个人信息处理活动。

风险评估的内容应当包括:

(一)个人信息的处理目的、处理方式等是否合法、正当、必要;

(二)对个人的影响及风险程度;

(三)所采取的安全保护措施是否合法、有效并与风险程度相适应。风险评估报告和处理情况记录应当至少保存三年。

第五十六条个人信息处理者发现个人信息泄露的,应当立即采取补救措施,并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项:

(一)个人信息泄露的原因;

(二)泄露的个人信息种类和可能造成的危害;

(三)已采取的补救措施;

(四)个人可以采取的减轻危害的措施;

(五)个人信息处理者的联系方式。

个人信息处理者采取措施能够有效避免信息泄露造成损害的,个人信息处理者可以不通知个人;但是,履行个人信息保护职责的部门认为个人信息泄露可能对个人造成损害的,有权要求个人信息处理者通知个人。

第五十七条提供基础性互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者,应当履行下列义务:

(一)成立主要由外部成员组成的独立机构,对个人信息处理活动进行监督;

(二)对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者,停止提供服务;

(三)定期发布个人信息保护社会责任报告,接受社会监督。

第五十八条接受委托处理个人信息的受托方,应当履行本章规定的相关义务,采取必要措施保障所处理的个人信息的安全。

第六章 履行个人信息保护职责的部门

第五十九条国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定,在各自职责范围内负责个人信息保护和监督管理工作。

县级以上地方人民政府有关部门的个人信息保护和监督管理职责,按照国家有关规定确定。

前两款规定的部门统称为履行个人信息保护职责的部门。

第六十条履行个人信息保护职责的部门履行下列个人信息保护职责:

(一)开展个人信息保护宣传教育,指导、监督个人信息处理者开展个人信息保护工作;

(二)接受、处理与个人信息保护有关的投诉、举报;

(三)调查、处理违法个人信息处理活动;

(四)法律、行政法规规定的其他职责。

第六十一条国家网信部门统筹协调有关部门依据本法推进下列个人信息保护工作:

(一)制定个人信息保护具体规则、标准;

(二)针对敏感个人信息以及人脸识别、人工智能等新技术、新应用,制定专门的个人信息保护规则、标准;

(三)支持研究开发安全、方便的电子身份认证技术;

(四)推进个人信息保护社会化服务体系建设,支持有关机构开展个人信息保护评估、认证服务。

第六十二条履行个人信息保护职责的部门履行个人信息保护职责,可以采取下列措施:况;

(一)询问有关当事人,调查与个人信息处理活动有关的情

(二)查阅、复制当事人与个人信息处理活动有关的合同、记录、账簿以及其他有关资料;查;

(三)实施现场检查,对涉嫌违法个人信息处理活动进行调

(四)检查与个人信息处理活动有关的设备、物品;对有证据证明是违法个人信息处理活动的设备、物品,向本部门主要负责人书面报告并经批准,可以查封或者扣押。

履行个人信息保护职责的部门依法履行职责,当事人应当予以协助、配合,不得拒绝、阻挠。

第六十三条履行个人信息保护职责的部门在履行职责中,发现个人信息处理活动存在较大风险或者发生个人信息安全事件的,可以按照规定的权限和程序对该个人信息处理者的法定代表人或者主要负责人进行约谈,或者要求个人信息处理者委托专业机构对其个人信息处理活动进行合规审计。个人信息处理者应当按照要求采取措施,进行整改,消除隐患。

第六十四条任何组织、个人有权对违法个人信息处理活动向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理,并将处理结果告知投诉、举报人。

履行个人信息保护职责的部门应当公布接受投诉、举报的联系方式。

第七章 法律责任

第六十五条违反本法规定处理个人信息,或者处理个人信息未按照规定采取必要的安全保护措施的,由履行个人信息保护职责的部门责令改正,给予警告,没收违法所得;拒不改正的,并处一百万元以下罚款;对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前款规定的违法行为,情节严重的,由履行个人信息保护职责的部门责令改正,没收违法所得,并处五千万元以下或者上一年度营业额百分之五以下罚款,并可以责令暂停相关业务、停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照;对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

第六十六条有本法规定的违法行为的,依照有关法律、行政法规的规定记入信用档案,并予以公示。

第六十七条国家机关不履行本法规定的个人信息保护义务的,由其上级机关或者履行个人信息保护职责的部门责令改正;对直接负责的主管人员和其他直接责任人员依法给予处分。

第六十八条个人信息权益因个人信息处理活动受到侵害,个人信息处理者不能证明自己没有过错的,应当承担损害赔偿等侵权责任。前款规定的损害赔偿责任按照个人因此受到的损失或者个人信息处

理者因此获得的利益确定;个人因此受到的损失和个人信息处理者因此获得的利益难以确定的,根据实际情况确定赔偿数额。

第六十九条个人信息处理者违反本法规定处理个人信息,侵害众多个人的权益的,人民检察院、履行个人信息保护职责的部门和国家网信部门确定的组织可以依法向人民法院提起诉讼。

第七十条违反本法规定,构成违反治安管理行为的,依法给予治安管理处罚;构成犯罪的,依法追究刑事责任。

第八章 附则

第七十一条自然人因个人或者家庭事务处理个人信息的,不适用本法。法律对各级人民政府及其有关部门组织实施的统计、档案管理活动中的个人信息处理有规定的,适用其规定。

第七十二条本法下列用语的含义:

(一)个人信息处理者,是指自主决定处理目的、处理方式等个人信息处理事项的组织、个人。

(二)自动化决策,是指利用个人信息对个人的行为习惯、兴趣爱好或者经济、健康、信用状况等,通过计算机程序自动分析、评估并进行决策的活动。

(三)去标识化,是指个人信息经过处理,使其在不借助额外信息的情况下无法识别特定自然人的过程。

(四)匿名化,是指个人信息经过处理无法识别特定自然人且不能复原的过程。

第七十三条本法自年月日起施行。