



SESEC IV Selected Translation

Personal Information Protection Law

August | 2021

Introduction

On 20 August 2021, China passed the Personal Information Protection Law (PIPL), which lays out for the first time a comprehensive set of rules covering data processing. The release of the PIPL, which will take effect on 1 November 2021, completes the trifecta of China's foundational data governance regime – together with the Cybersecurity Law and the Data Security Law.

The translation selected by SESEC is as follows.

DISCLAIMER: This translation is produced by Pkulaw and may be used only for reference purposes. This English version is not an official translation of the original Chinese document by People's Congress of the People's Republic of China. In cases where any differences occur between the English version and the original Chinese version, the Chinese version shall prevail which can be found here. SESEC shall accept no responsibility or liability for damage or loss caused by any error, inaccuracy, or misunderstanding with regard to this translation.

Personal Information Protection Law

Table of Contents

Chapter I General Provisions

Chapter II Personal Information Processing Rules

Section 1 General Rules

Section 2 Rules on Processing Sensitive Personal Information

Section 3 Specific Provisions on the Processing of Personal Information by State Organs

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

Chapter IV Individuals' Rights in Personal Information Processing Activities

Chapter V Obligations of Personal Information Processors

Chapter VI Departments Performing Personal Information Protection Functions

Chapter VII Legal Liability

Chapter VIII Supplemental Provisions

Chapter I General Provisions

Article 1 For the purposes of protecting rights and interests relating to personal information, regulating personal information processing activities, and promoting the reasonable use of personal information, this Law is enacted in accordance with the Constitution.

Article 2 The personal information of natural persons shall be protected by law. No organization or individual may infringe upon natural persons' rights and interests relating to personal information.

Article 3 This Law shall apply to the processing, within the territory of the People's Republic of China, of the personal information of natural persons.

This Law shall also apply to the processing outside the territory of the People's Republic of China of the personal information of natural persons within the territory of the People's Republic of China if the information is processed:

- (1) for the purpose of providing products or services to natural persons inside China;
- (2) to analyze or assess the conduct of natural persons inside China; or
- (3) under any other circumstance as provided by any law or administrative regulation.

Article 4 "Personal information" means all kinds of information relating to identified or identifiable natural persons recorded by electronic or other means, excluding anonymized information.

Personal information processing includes personal information collection, storage, use, processing, transmission, provision, disclosure, and deletion, among others.

Article 5 Personal information shall be processed under the principles of lawfulness, propriety, necessity and good faith, and may not be processed by misleading, fraud, coercion or other means.

Article 6 Personal information shall be processed for a clear and reasonable purpose which is directly related to the processing purpose and in the manners that have the minimum impacts on the rights and interests of individuals.

Personal information shall be collected within the smallest scope required for achieving the processing purpose, and excessive collection of personal information is forbidden.

Article 7 The principles of openness and transparency shall be observed in the processing of personal information, the rules for the processing of personal information shall be disclosed to the public, and the purposes, methods, and scope of information processing shall be explicitly indicated.

Article 8 The quality of personal information shall be guaranteed in the processing of personal information to avoid adverse impacts on the rights and interests of individuals caused by inaccurate and incomplete personal information.

Article 9 Personal information processors shall be responsible for their personal information processing activities, and take necessary measures to guarantee the security of the personal information they process.

Article 10 No organization or individual may illegally collect, use, process, or transmit the personal information or illegally buy or sell, provide, or publish the personal information of other persons; or engage in personal information processing activities compromising national security or public interests.

Article 11 The state shall establish and improve the personal information protection system to prevent and severely punish infringements of rights and interests relating to personal information, strengthen publicity and education on personal information protection, and promote the formation of a good environment for the joint participation in personal information protection by the government, enterprises, relevant social organizations, and the public.

Article 12 The state shall vigorously participate in the development of international rules on personal information protection, boost international exchange and cooperation in terms of personal information protection, and promote the mutual recognition of personal information protection rules and standards, among others, between China and other countries, regions, and international organizations.

Chapter II Personal Information Processing Rules

Section 1 General Rules

Article 13 A personal information processor may not process personal information unless:

- (1) the individual's consent has been obtained;
- (2) the processing is necessary for the conclusion or performance of a contract to which the individual is a party or for conducting human resource management in accordance with the labor rules and regulations developed according to the law and the collective contract signed according to the law.
- (3) the processing is necessary to fulfill statutory functions and statutory obligations;
- (4) the processing is necessary to respond to public health emergencies or protect natural persons' life, health and property safety under emergency circumstances;
- (5) personal information is processed within a reasonable scope to conduct news reporting, public opinion-based supervision, and other activities in the public interest;

(6) the personal information that has been published by the individuals themselves or other personal information that has been legally published is processed within a reasonable scope in accordance with this Law; or

(7) under any other circumstance as provided by any law or regulation.

In accordance with other relevant provisions of this Law, an individual's consent shall be obtained before processing his or her personal information, except under the circumstances specified in subparagraphs (2) to (7) of the preceding paragraph.

Article 14 Where personal information is processed based on an individual's consent, such consent shall be expressed by the individual voluntarily and explicitly on the premise of being fully informed. Where any law or administrative regulation provides that the individual's separate consent or written consent shall be obtained for processing personal information, such provision shall prevail.

In the case of any change of the purpose of the processing of personal information, the processing method, or the category of processed personal information, the individual's consent shall be obtained again.

Article 15 Where personal information is processed based on an individual's consent, the individual shall have the right to withdraw his or her consent. The personal information processor shall provide convenient ways to withdraw the consent.

The individual's withdrawal of his or her consent does not affect the effectiveness of personal information processing activities that have been conducted based on his or her consent before the withdrawal of such consent.

Article 16 A personal information processor may not refuse to provide products or services on the ground that the relevant individual does not consent to the processing of his or her personal information or withdraws consent, except that the processing of personal information is necessary for the provision of products or services.

Article 17 A personal information processor shall, before processing personal information, authentically, accurately and completely notify individuals of the following matters in a conspicuous way and using clear and easily understood language:

- (1) The title or name and contact information of the personal information processor.
- (2) Purposes of the processing of personal information, processing methods, categories of the processed personal information, and the preservation periods.
- (3) Methods and procedures for individuals to exercise the rights provided in this Law.
- (4) Other matters that should be notified as provided by laws and administrative regulations.

Where any matter as set forth in the preceding paragraph changes, the individual shall be notified of the change.

Where the personal information processor notifies the matters as set forth in paragraph 1 in the method of developing personal information processing rules, the processing rules shall be disclosed to the public and easy to consult and preserve.

Article 18 Personal information processors processing personal information are permitted not to notify individuals of the matters as set forth in paragraph 1 of the preceding article if laws or administrative regulations provide that such processing shall be kept confidential or notification is not necessary.

Where it is impossible to notify individuals in a timely manner for the protection of natural persons' life, health and property safety under emergency circumstances, personal information processors shall notify them in a timely manner after the elimination of the emergency circumstances.

Article 19 A preservation period of personal information shall be the shortest time necessary to achieve the processing purpose, except as otherwise provided for by any law or administrative regulation.

Article 20 Where two or more personal information processors jointly decide on the purposes of the processing of personal information and processing methods, they shall agree on their respective rights and obligations. However, such agreement does not affect an individual's request for exercising his or her rights as provided in this Law filed with any of the said personal information processors.

Where personal information processors jointly processing personal information infringe the rights and interests relating to personal information, causing damages, they shall bear joint and several liability according to the law.

Article 21 A personal information processor entrusting the processing of personal information shall agree with the entrusted party on the purposes and period of the entrusted processing, processing methods, categories of personal information, protection measures, as well as the rights and obligations of both parties, among others, and conduct supervision of the personal information processing activities of the entrusted party.

The entrusted party shall process personal information as agreed, and may not process personal information beyond the agreed processing purposes or processing methods, among others. Where the entrustment contract has not taken effect or is null and void, revoked, or rescinded, the entrusted party shall return personal information to the personal information processor or delete it, and shall not retain such information.

Without the consent of the personal information processor, the entrusted party may not sub-entrust the processing of personal information to any other party.

Article 22 Where a personal information processor needs to transfer personal information due to combination, division, dissolution or declaration of bankruptcy, among others, it or he shall inform individuals of the title or name and contact information of the recipient. The recipient shall continue to perform the obligations of the personal information processor. If the recipient changes the original processing purposes or processing methods, it or he shall obtain the individuals' consent again in accordance with this Law.

Article 23 A personal information processor that provides any other personal information processor with the personal information it or he processes shall notify individuals of the recipient's title or name, contact information, processing purposes, processing methods, and categories of personal information, and obtain the individuals' separate consent. The recipient shall process personal information within the scope of the aforementioned processing purposes, processing methods, and categories of personal information, among others. Where the recipient changes the original processing purposes or processing methods, it or he shall obtain individuals' consent again in accordance with this Law.

Article 24 Where a personal information processor conducts automated decision making by using personal information, it or he shall ensure the transparency of the decision making and the fairness and impartiality of the result, and may not give unreasonable differential treatment to individuals in terms of trading price or other trading conditions.

Where information push or commercial marketing is conducted by means of automated decision making, options not specific to individuals' characteristics shall be provided simultaneously, or convenient ways to refuse shall be provided to individuals.

Where a decision significantly affecting an individual's rights and interests is made in the manner of automated decision making, the individual shall have the right to require the personal information processor to make explanations and to refuse that the personal information processor makes decisions solely in the manner of automated decision making.

Article 25 Personal information processors may not disclose to the public the personal information they process, except with the separate consent of individuals.

Article 26 The installation of image collection or personal identification equipment in public places shall be necessary for maintaining public security and comply with relevant provisions issued by the state, and conspicuous signs shall be erected. The collected personal images and identification information can only be used for the purpose of maintaining public security, and shall not be used for other purposes, except with the separate consent of individuals.

Article 27 A personal information processor may process the personal information that has been published by an individual himself or herself or the personal information that has been legally published within a reasonable scope, except that the individual has expressly refused. Where the personal information that has been made public by a personal information processor significantly affects an individual's rights and interests, the individual's consent shall be obtained in accordance with this Law.

Section 2 Rules on Processing Sensitive Personal Information

Article 28 "Sensitive personal information" means personal information that, once leaked or illegally used, may easily result in the trampling of the personal dignity of natural persons or endanger personal or property security, including information on biometric identification, religious beliefs, specific identity, medical health, financial accounts, and personal whereabouts, among others, and personal information of minors under the age of fourteen.

Personal information processors may not process sensitive personal information unless there are specific purposes and sufficient necessity and strict protection measures are taken.

Article 29 An individual's separate consent shall be obtained before processing his or her sensitive personal information. Where any law or administrative regulation provides that written consent shall be obtained for processing sensitive personal information, such provision shall prevail.

Article 30 To process sensitive personal information, personal information processors shall inform individuals of the necessity of the processing of sensitive personal information and the impacts on individuals' rights and interests in addition to the matters specified in paragraph 1 of Article 17 of this Law, except that it is not necessary to inform the individuals of such information according to this Law.

Article 31 Where a personal information processor processes the personal information of a minor under the age of fourteen, it or he shall obtain the consent of the minor's parents or other guardians.

A personal information processor that processes the personal information of a minor under the age of fourteen shall develop special personal information protection rules.

Article 32 Where any law or administrative regulation provides that the processing of sensitive person information shall be subject to relevant administrative licensing or other restrictions, such provisions shall prevail.

Section 3 Specific Provisions on the Processing of Personal Information by State Organs

Article 33 This Law shall apply to the processing of personal information by state organs. Where there are any special provisions in this Section, such provisions shall prevail.

Article 34 State organs processing personal information to fulfill their statutory functions shall process such information according to the authority and procedures provided in laws and administrative regulations, and may not do so in excess of the scope necessary to fulfill their statutory functions and the limits.

Article 35 State organs processing personal information to fulfill their statutory functions shall fulfill the obligation of notification according to the provisions of this Law, except that there is any circumstance as prescribed in paragraph 1 of Article 18 of this Law or notification will impede state organs' fulfillment of their statutory functions.

Article 36 Personal information processed by state organs shall be stored within the territory of the People's Republic of China; and where it is necessary to provide such information abroad, security assessment shall be conducted. Relevant departments may be required to provide support and assistance for security assessment.

Article 37 Where organizations that are authorized by laws and regulations to exercise the power of administering public affairs process personal information to fulfill their statutory functions, the provisions of this Law on the processing of personal information by state organs shall apply.

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

Article 38 Where a personal information processor truly needs to provide personal information to any party outside the territory of the People's Republic of China for business needs, among others, it or he shall meet any of the following conditions:

- (1) Security assessment organized by the national cyberspace administration has been passed in accordance with Article 40 of this Law.
- (2) Personal information protection certification has been conducted by a specialized institution according to provisions issued by the national cyberspace administration.
- (3) A contract has been concluded with the overseas recipient based on the model contract developed by the national cyberspace administration, agreeing on both parties' rights and obligations.
- (4) Other conditions provided in laws or administrative regulations or by the national cyberspace administration.

Where any international treaty or agreement concluded or acceded to by the People's Republic of China provides for the conditions on the provision of personal information to any party outside the territory of the People's Republic of China, such provisions may apply.

The personal information processor shall take necessary measures to ensure that personal information processing activities of the overseas recipient meet the personal information protection standards provided in this Law.

Article 39 Where a personal information processor provides personal information to any party outside the territory of the People's Republic of China, it or he shall notify individuals of the overseas recipient's title or name, contact information, processing purposes, processing methods, categories of personal information, the methods of and procedures for individuals' exercise of the rights provided in this Law over the overseas recipient, and other matters, and obtain individuals' separate consent.

Article 40 Critical information infrastructure operators and the personal information processors that process the personal information reaching or exceeding the threshold specified by the national cyberspace administration in terms of quantity shall store domestically the personal information collected and generated within the territory of the People's Republic of China. Where it is truly necessary to provide the information abroad, the security assessment organized by the national cyberspace administration shall be passed. Where laws, administrative regulations, or provisions issued by the national cyberspace administration provide that security assessment is not necessary, such provisions shall prevail.

Article 41 The competent authority of the People's Republic of China shall process a request for personal information stored within the territory of the People's Republic of China from a foreign judicial or law enforcement authority in accordance with relevant laws and international treaties and agreements entered into or acceded to by the People's Republic of China, or under the principle of equality and reciprocity. Without the approval of the competent authority of the People's Republic of China, a personal information processor shall not provide personal information stored within the territory of the People's Republic of China to any foreign judicial or law enforcement authority.

Article 42 Where an overseas organization or individual engages in personal information processing activities that infringes the rights and interests relating to personal information of citizens of the People's Republic of China or compromise national security or public interests of the People's Republic of China, the national cyberspace administration may include it or him in a list of those the provision of personal information to whom is restricted or prohibited, make an announcement, and take measures such as restricting or prohibiting the provision of personal information to it or him.

Article 43 Where any country or region adopts any prohibitive, restrictive or other similar discriminatory measures against the People's Republic of China in terms of personal information protection, the People's Republic of China may take reciprocal measures against the aforesaid country or region according to the actual circumstances.

Chapter IV Individuals' Rights in Personal Information Processing Activities

Article 44 Individuals shall have the right to know and the right to decide on the processing of their personal information, and have the right to restrict or refuse the processing of their personal information by others, except as otherwise provided by any law or administrative regulation.

Article 45 Individuals shall have the right to consult and duplicate their personal information from personal information processors, except under circumstances as set out in paragraph 1 of Article 18 or Article 35 of this Law.

Where individuals request the consultation or duplication of their personal information, personal information processors shall provide such information in a timely manner.

Where individuals request the transfer of personal information to their designated personal information processors, and the conditions specified by the national cyberspace authority are met, personal information processors shall provide the channels for transfer.

Article 46 Where individuals discover that their personal information is incorrect or incomplete, they shall have the right to request personal information processors to correct or supplement relevant information.

Where individuals request the correction or supplementation of their personal information, personal information processors shall verify the personal information, and correct or supplement relevant information in a timely manner.

Article 47 Under any of the following circumstances, a personal information processor shall voluntarily delete an individual's personal information; and, if the personal information processor fails to delete such information, the individual shall have the right to request it or him to do so:

- (1) The processing purpose has been achieved or cannot be achieved, or it is no longer necessary to achieve the processing purpose.
- (2) The personal information processor ceases the provision of products or services, or the preservation period has expired.
- (3) The individual withdraws consent.
- (4) The personal information processor processes personal information in violation of any law or administrative regulation or the agreement.
- (5) Other circumstances as provided by laws and administrative regulations.

Where the preservation period provided by any law or administrative regulation has not expired, or it is difficult to realize the deletion of personal information technically, the personal information processor shall cease the processing of personal information other than storing and taking necessary security protection measures for such information.

Article 48 Individuals shall have the right to request personal information processors to interpret the personal information processing rules they develop.

Article 49 Where a natural person dies, his or close relatives may, for their own legitimate and appropriate rights and interests, exercise the rights to consult, duplicate, correct and delete the relevant personal information of the deceased, among others, except as otherwise arranged by the deceased before his or her death.

Article 50 Personal information processors shall establish the convenient mechanisms for accepting and handling individuals' applications for exercising their rights. If an individual's request for exercising his or her rights is rejected, the reasons therefor shall be given.

Where a personal information processor rejects an individual's request for exercising his or her rights, the individual may file a lawsuit with the people's court according to the law.

Chapter V Obligations of Personal Information Processors

Article 51 Personal information processors shall, on the basis of the purposes of the processing of personal information, processing methods, categories of personal information, the impacts on individuals' rights and interests, and potential security risks, among others, take the following measures to ensure that personal information processing activities comply with the provisions of laws and administrative regulations, and prevent unauthorized access to as well as the leakage, tampering or loss of personal information:

- (1) Developing internal management rules and operating procedures.
- (2) Conducting classified management of personal information.
- (3) Taking corresponding security technical measures such as encryption and de-identification.
- (4) Determining in a reasonable manner the operation privileges relating to personal information processing, and providing security education and trainings for employees on a regular basis.
- (5) Developing and organizing the implementation of emergency plans for personal information security incidents.
- (6) Other measures as provided by laws and administrative regulations.

Article 52 A personal information processor that processes the personal information reaching or exceeding the threshold specified by the national cyberspace administration in terms of quantity shall appoint a person in charge of personal information protection to be responsible for conducting supervision of personal information processing activities as well as the protection measures taken, among others.

The personal information processor shall publish the contact information of the person in charge of personal information protection, and submit the name and contact information, among others, of the person in charge of personal information protection to the department performing personal information protection functions.

Article 53 Personal information processors outside the territory of the People's Republic of China as provided in paragraph 2 of Article 3 of this Law shall establish special institutions or designate representatives within the territory of the People's Republic of China to handle affairs relating to personal information protection, and submit the names of relevant institutions or the names and contact information, among others, of representatives to the departments performing personal information protection functions.

Article 54 Personal information processors shall audit on a regular basis the compliance of their processing of personal information with laws and administrative regulations.

Article 55 Under any of the following circumstances, personal information processors shall conduct personal information protection impact assessment in advance, and record the processing information:

- (1) Processing sensitive personal information.
- (2) Using personal information to conduct automated decision making.

(3) Entrusting personal information processing, providing personal information to other personal information processors, or disclosing personal information to the public.

(4) Providing personal information abroad.

(5) Other personal information processing activities which have significant impacts on individuals' rights and interests.

Article 56 The content of personal information protection impact assessment shall include:

(1) Whether the purposes of the processing of personal information and processing methods, among others, are lawful, justified and necessary.

(2) The impacts on individuals' rights and interests and security risks.

(3) Whether the protection measures taken are lawful, effective, and commensurate with the degrees of risks.

Personal information protection impact assessment reports and records on processing shall be preserved for at least three years.

Article 57 Where leakage, tampering or loss of personal information occurs or may occur, a personal information processor shall immediately take remedial measures, and notify the department performing personal information protection functions and the relevant individuals. The notice shall include the following matters:

(1) The categories of personal information that is or may be leaked, tampered with or lost, and the causes and possible harm of the leakage, tampering or loss of the personal information.

(2) Remedial measures taken by the personal information processor and measures the individuals may take to mitigate the harm.

(3) The contact information of the personal information processor.

Where the measures taken by the personal information processor can effectively avoid the harm created by information leakage, tampering or loss, the personal information processor is allowed not to notify individuals; and where the department performing personal information protection functions considers that harm may be caused, it shall have the right to require the personal information processor to notify individuals.

Article 58 Personal information processors that provide important Internet platform services involving a huge number of users and complicated business types shall perform the following obligations:

(1) Establishing and improving the system of personal information protection compliance rules in accordance with the provisions issued by the state, forming independent institutions mainly consisting of external personnel to supervise personal information protection.

(2) Following the principles of openness, fairness and impartiality, developing platform rules, and clarifying the norms for the processing of personal information by product or service providers on platforms and the obligations to protect personal information.

(3) Stopping providing services to product or service providers on platforms that process personal information in severe violation of laws and administrative regulations.

(4) Issuing social responsibility reports on personal information protection on a regular basis to be subject to public supervision.

Article 59 The parties that are entrusted with the processing of personal information shall, in accordance with the provisions of this Law and relevant laws and administrative regulations, take necessary measures to ensure the security of the personal information processed, and assist personal information processors in fulfilling the obligations specified in this Law.

Chapter VI Departments Performing Personal Information Protection Functions

Article 60 The national cyberspace administration shall be responsible for the overall planning and coordination of personal information protection work and related supervision and administration. Relevant departments of the State Council shall, in accordance with this Law and relevant laws and administrative regulations, be responsible for personal information protection and the supervision and administration thereof within the scope of their respective functions.

The personal information protection and supervision and administration functions of the relevant departments of the local people's governments at or above the county level shall be determined in accordance with the relevant provisions issued by the state.

The departments specified in the preceding two paragraphs shall be collectively referred to as departments performing personal information protection functions.

Article 61 Departments performing personal information protection functions shall perform the following personal information protection functions:

- (1) Conducting publicity and education on personal information protection, and guiding and supervising the personal information protection conducted by personal information processors.
- (2) Accepting and processing complaints and reports relating to personal information protection.
- (3) Organizing the testing and assessment of the personal information protection of application programs, among others, and publishing the testing and assessment results.
- (4) Investigating and processing illegal personal information processing activities.
- (5) Other functions as provided by laws and administrative regulations.

Article 62 The national cyberspace administration shall coordinate the efforts of relevant departments to promote the following personal information protection work in accordance with this Law:

- (1) Developing specific rules and standards for personal information protection.
- (2) Developing special personal information protection rules and standards for small-sized person information processors, processing of sensitive personal information, and new technologies and applications such as facial recognition and artificial intelligence.
- (3) Supporting the research, development, promotion and application of safe and convenient electronic identity authentication technologies, and promoting the development of public services for online identity authentication.
- (4) Advancing the construction of a socialized service system for personal information protection, and supporting relevant institutions in providing personal information protection assessment and certification services.

(5) Improving the working mechanisms for personal information protection complaints and reports.

Article 63 When performing personal information protection functions, the departments performing personal information protection functions may take the following measures:

- (1) Interviewing relevant parties, and investigating circumstances relating to personal information processing activities.
- (2) Consulting and duplicating the parties' contracts, records, account books and other relevant materials relating to personal information processing activities.
- (3) Conducting on-site inspections, and conducting investigations of suspected illegal personal information processing activities.
- (4) Inspecting equipment and articles relating to personal information processing activities; and seizing or impounding equipment and articles used for illegal personal information processing activities as proved by evidence after submitting written reports to and obtaining approval from the primary persons-in-charge of these departments.

When departments performing personal information protection functions perform their functions according to the law, the parties shall provide assistance and cooperation, and shall not reject or obstruct them.

Article 64 Where a department performing personal information protection functions finds during the performance of its functions that there are relatively large risks in personal information processing activities or any personal information security incident occurs, it may hold an interview with the legal representative or primary person in charge of the personal information processor according to specified authority and procedures, or require the personal information processor to authorize a professional institution to audit the regulatory compliance of its or his personal information processing activities. The personal information processor shall adopt measures, make rectification and eliminate hidden risks as required.

Where a department that performs personal information protection functions finds during the performance of its functions that any illegal processing of personal information is suspected of constituting a crime, it shall transfer the case to the public security organ for handling according to the law in a timely manner.

Article 65 All organizations and individuals shall have the right to file complaints or reports about illegal personal information processing activities with departments performing personal information protection functions. The departments receiving complaints or reports shall handle them without delay according to the law, and notify the complainants and informants of the handling results.

The departments performing personal information protection functions shall publish the contact information for accepting complaints and reports.

Chapter VII Legal Liability

Article 66 Where a personal information processor processes personal information in violation of this Law or fails to fulfill the personal information protection obligations as provided in this Law in the process of processing personal information, the department performing personal information protection functions shall order the personal information processor to take corrective action, give it or

him a warning, and confiscate its or his illegal income; and where any application programs process personal information in violation of laws, the department performing personal information protection functions shall order the suspension or termination of provision of services by such application programs. If the personal information processor refuses to take corrective action, it or he shall be fined not more than one million yuan; and the directly liable person in charge and other directly liable persons shall each be fined not less than 10,000 yuan nor more than 100,000 yuan.

Where a personal information processor commits any illegal conduct as specified in the preceding paragraph with serious circumstances, the department performing personal information protection functions at or above the provincial level shall order it or him to take corrective action, confiscate its or his illegal income, and impose a fine of not more than 50 million yuan or not more than 5% of the turnover in the previous year, and may order the suspension of relevant business or cessation of business operations for an overhaul, and notify the relevant competent department to revoke the relevant business permit or business license; and impose a fine of not less than 100,000 yuan nor more than one million yuan on each of the directly liable person in charge and other directly liable persons, and may decide to prohibit them from serving as directors, supervisors, senior executives or persons in charge of personal information protection of related enterprises during a certain period of time.

Article 67 Where any violation of laws as prescribed in this Law is committed, it shall be entered into the relevant credit record and be published in accordance with the provisions of the relevant laws and administrative regulations.

Article 68 Where any state organ fails to fulfill the personal information protection obligations as provided in this Law, the superior organ or the department performing personal information protection functions shall order it to take corrective action, and take disciplinary action against directly liable person in charge and other directly liable persons according to the law.

Where any functionary of the department performing personal information protection functions neglects duty, abuses power, or makes falsification for private gain, which is not criminally punishable, he or she shall be subject to disciplinary action according to the law.

Article 69 Where personal information processing infringes rights and interests relating to personal information, causing damages, and the personal information processor cannot prove that it or he is not at fault, the personal information processor shall assume liability for damages and other tort liability.

The “liability for damages” provided in the preceding paragraph shall be determined based the losses incurred by individuals thereby or the benefits obtained by the personal information processor therefrom; and where it is difficult to determine the losses incurred by individuals thereby or the benefits obtained by the personal information processor therefrom, the amount of damages shall be determined according to the actual circumstances.

Article 70 Where a personal information processor processes personal information in violation of the provisions of this Law, infringing the rights and interests of many individuals, the people's procuratorate, the consumer organization as provided by any law, or the organization determined by the national cyberspace administration may file a lawsuit with the people's court according to the law.

Article 71 Where any violation of this Law constitutes a violation of public security administration, the public security administration punishment shall be imposed according to the law; and if the violation constitutes a crime, the violator shall be held criminally liable according to the law.

Chapter VIII Supplemental Provisions

Article 72 This Law shall not apply when a natural person processes personal information for personal or household affairs.

Where laws provide for the personal information processing in the process of statistical or archives administration activities organized and implemented by the people's governments at all levels and relevant departments, such provisions shall prevail.

Article 73 For the purposes of this Law, the following terms shall have the following meanings:

(1) “Personal information processor” means an organization or individual that independently decides on the processing purposes and processing methods during personal information processing activities.

(2) “Automated decision making” means the activities of automatically analyzing and assessing individuals' behavioral habits, hobbies, or financial, health and credit status, among others, through computer programs and making decisions thereon.

(3) “De-identification” means the process of processing personal information to make it impossible to identify specific natural persons without the support of additional information.

(4) “Anonymization” means the process of processing personal information to make it impossible to identify specific natural persons and impossible to restore.

Article 74 This Law shall come into force on November 1, 2021.

20 August 2021

People's Congress of the People's Republic of China

Introduction of SESEC Project



The Seconded European Standardization Expert in China (SESEC) is a visibility project co-financed by the European Commission (EC), the European Free Trade Association (EFTA) secretariat and the three European Standardization Organizations (CEN, CENELEC and ETSI). Since 2006, there has been three SESEC projects in China, SESEC I (2006-2009), SESEC II (2009- 2012) and SESEC III (2014-2017). In April 2018, SESEC IV was officially launched in Beijing, China. Dr. Betty XU was nominated as the SESEC expert and will spend the next 36 months on promoting EU-China standardization information exchange and EU-China standardization cooperation.

The SESEC project supports the strategic objectives of the European Union, EFTA and the European Standardization Organizations (ESOs). The purpose of SESEC project is to:

- **Promote European and international standards in China;**

- **Improve contacts with different levels of the Chinese administration, industry and standardization bodies;**
- **Improve the visibility and understanding of the European Standardization System (ESS) in China;**
- **Gather regulatory and standardization intelligence.**

The following areas have been identified as sectorial project priorities by the SESEC project partners: Internet of Things (IoT) & Machine-to-Machine(M2M) communication, communication networks & services, cybersecurity & digital identity, Smart Cities (including transport, power grids & metering), electrical & electronic products, general product safety, medical devices, cosmetics, energy management & environmental protection (including eco-design & labelling, as well as environmental performance of buildings).