Brief Comments on the Personal Information Protection Law

Authors: Kevin DUAN | Kemeng CAI | Tina WANG | Minzhe HU

On August 20, 2021, the *Personal Information Protection Law of the People's Republic of China* (the "**PIPL**") was officially promulgated, which will come into effect on November 1, 2021. The PIPL will become the first systematic and comprehensive law in China that focuses on the protection of personal information.

The final draft of the PIPL (the "**Final Draft**"), on the basis of the second reading draft (the "**Second Reading Draft**"), further strengthens the requirements for personal information protection and improves the legal bases for personal information processing. The Final Draft also emphasizes the provisions on "big data discrimination" and "right to data portability" in the context of ensuring the orderly development of the platform economy, and further strengthens protections for the rights of personal information subjects and the public interest. In addition to administrative supervision, the Final Draft also further strengthens the provisions on personal litigation rights and public interest litigation. These diversified means for personal information subjects to protect their rights will further enhance the deterrence effect of the PIPL.

However, the Final Draft also takes into account the operability and feasibility of these regulations, includes human resources management as a legal basis for processing, and adds concepts such as "small personal information handler". It moderately relaxes restrictions on processing public personal information, and improves certain provisions in light of specific scenarios.

If the Cybersecurity Law opened a new stage for personal information protection in China, the PIPL brings personal information protection into a new era. Its fundamental institutional framework and wide application will have a profound impact on the digital society, including online retail, artificial intelligence, autonomous driving, healthcare, and the Internet of Things.

We will analyze and interpret the PIPL in light of the major changes in the Final Draft.

Key revisions in the Final Draft compared to the Second Reading Draft

The key revisions in the Final Draft compared to the Second Reading Draft include the following:

- Improves the legal bases for personal information processing, includes human resources management as a legal basis for processing, and further defines the applicable scope of the legal basis for processing public information;
- Points out "big data discrimination", strengthen the supervision of automatic decision making, and protects the rights of individuals to obtain fair transaction terms;
- Further limits the conditions for processing sensitive personal information to "only for a specific purpose and sufficient necessity, and subject to strict protection measures";
- Grants individuals the "right to data portability", strengthens individuals' control over their personal information, and protects the free flow of personal information between different platforms;
- Strengthens the supervision of mobile applications;
- Raises for the first time the concept of "small personal information handler", which lays a regulatory foundation for potentially exempting small enterprises from certain personal information obligations;
- Protects individuals' litigation rights by specifying actionability when personal information handlers refuse individuals' requests to exercise their personal information rights, including consumer organizations in the public interest litigation system.

Processing based on human resources management and processing public information: further adjustments to multiple legal bases for personal information processing

The PIPL adds several legal bases for processing personal information, including "necessary to perform a contract to which an individual is a party", "necessary to perform a legal obligation", etc. This is a breakthrough compared to the Cybersecurity Law, in which consent is the only legal basis for processing. The PIPL provides more diverse legal bases for the processing of personal information. It is worth noting that while the multiple legal bases alleviate the rigid application of the "informed consent" principle, the "informed consent" requirement is, in fact, enhanced. The requirement for "consent" can only be deemed to be satisfied when the personal information subject can make a true and effective decision.

On the basis of the Second Reading Draft, the Final Draft adds human resources management as a legal basis for processing personal information, and optimizes the rules for processing public personal information.

I Human resources management

The PIPL's broad application toward a variety of personal information processing activities is reflected in the protection of employees' personal information, which has been neglected in practice and difficult to address under other laws, such as the Cybersecurity Law, the Law on the Protection of Rights and Interests of Consumers. Article 13.2 of the Final Draft further specifies that "human resources management" is a legal basis for processing personal information. However, this legal basis is strictly limited to that which is "necessary for implementing human resources management in conformity with the labor rules and regulations formulated in accordance with the law and the lawfully signed collective

contracts."

The emphasis on "the labor rules and regulations formulated in accordance with the law and the lawfully signed collective contracts" reflects that lawmakers have taken into account inequalities inherent in labor relations by attempting to strictly limit the scope of processing employees' personal information, and prevent employers from over-collecting employees' personal information by invoking "human resources management". On the other hand, this provision indicates a means for employers to lawfully process employees' personal information. Employers will not need to obtain each individual employee's consent if they collect personal information in conformity with internal labor rules and regulations that have been formulated through required democratic procedures in accordance with Article 4 of the Employment Contract Law.

With the enactment of the PIPL, employers will need to pay more attention to protecting employees' personal information in the same way that they treat users' personal information. We suggest that employers improve their internal labor rules and regulations as soon as possible to include provisions on the protection of employees' personal information. Employers should also pay attention to improving the mechanism for employees to exercise their rights to personal information because the PIPL grants a wide range of rights to personal information subjects, which may become a useful source of leverage for employees in potential labor disputes.

II Rules for processing public personal information

Article 27 of the Final Draft of the PIPL permits personal information handlers to "process, to a reasonable extent, personal information that the individual himself has made public or otherwise has been lawfully made public, unless the individual expressly refuses to do so. Where a personal information handler processes any public personal information, which has a significant impact on an individual's rights and interests, the individual's consent shall be obtained in accordance with this law." Compared with the Second Reading Draft, the wording in this revised article is more consistent with Article 1036.2 of the Civil Code[1]. Therefore, if personal information handlers wish to use personal information collected from public sources, it should select information that is made public by the individual or other lawfully public information (such as relevant information lawfully made public by various government websites and information made public in public news reports).

In addition, with respect to the method of processing public personal information, Article 27 of the Final Draft significantly simplifies the content and requirements under the Second Reading Draft, which would have required personal information handlers to judge the "the purpose why the personal information was made public" or "reasonably and prudently process the personal information when the purpose is unclear". However, processing of public personal information should still be "reasonable". When determining the scope of what is "reasonable", factors should be considered such as the purpose of making the personal information public, the individual's expectation of privacy, the impact of using

[1] Article 1036.2, under any of the following circumstances, an actor shall not bear civil liability… (2) the actor reasonably processes the information made public by the natural person himself or other information that has already been legally made public, unless the said person explicitly refuses or the processing of the information infringes on a significant interest of the person.

the public information on an individual's rights and interests, etc. Specific standards are yet to be specified by law enforcement and judicial decisions[2].

Big data discrimination and personalized marketing: norms and limitations for automated decision making

According to Article 73 of the PIPL, automated decision making refers to "an activity through a computer program to automatically analyze and evaluate a person's behavioral habits, hobbies, or financial, health, or credit status, etc., and to make decisions." Automated decision making is often used in information pushes, commercial marketing, credit reviews, job applicant personality assessments, employee performance assessments, etc. With respect to automated decision making, Article 24 of the PIPL requires that:

(1) The transparency of decisions and fair and just results of decisions shall be ensured, and no unreasonable differential treatment may be applied to individuals with respect to transaction terms, such as price.

(2) For information push, commercial marketing to individuals through automated decision making should also provide options that are not specific to their personal characteristics or provide a **convenient** way to refuse.

(3) For decisions that have a significant impact on an individual's rights and interests are made through automated decision making, an individual has the right to request an explanation from the personal information handler, and to refuse decisions made by the personal information handler solely through automated decision making.

I Big data discrimination

Paragraph (1), above, is mainly aimed at the much-criticized "big data discrimination." "Big data discrimination" generally refers to different pricing strategies that platforms adopt which target "frequent customers" with purchase records, users judged to be price-insensitive through big data analysis, and other specific types of individuals, which usually results in higher prices for "frequent customers" than "new customers".

[2] For example, in a personality rights dispute case heard by Beijing Internet Court in 2019, the plaintiff's identification photo published on the alumni social network website was placed on the photo search results of an industry-leading search engine. The court considered the nature of the information publishing platform, and held that the plaintiff's purpose of publishing information on the social network was to socialize within a specified group of people, rather than publishing it as public information on the network. In another case, the plaintiff claimed that the website infringed his privacy and other rights by forwarding the judgment that was published on the official website for publishing court decisions. In this case, the court balanced the public interest, socioeconomic interest and individual's interest, and considered the form and purpose of how defendant's website uses the public information. The court held that the defendant did not improperly tamper with the content of the judgment published on the official website, nor did it carry out data matching and information processing for improper purposes such as collecting the credit information of natural persons and prying into personal privacy. The purpose of the defendant's website republishing was not contrary to the purpose of judicial publicity. The court ultimately did not support the plaintiff's claims. In an administrative enforcement case regarding personal information rights where a company in Hangzhou infringed a consumer's right to personal information, the law enforcement authority held that the party infringed the consumer's personal information rights, which were legally protected, by using personal information collected from Qi Cha Cha, Qi Xin Bao and other apps to carry out marketing activities without the consent of the person.

Shortly before the promulgation of the Final Draft of the PIPL, the State Administration for Market Regulation promulgated the *Provisions on Administrative Penalties for Price-related Illegal Activities (Revision Draft for Comment)*[3], the *Provisions on the Prohibition of Unfair Internet Competition (Draft for Comments)*[4] and other regulations to regulate similar infringements of consumers' right to know and right to fair trade from the perspectives of price discrimination, unfair competition online, etc. The PIPL will also regulate differentiated pricing that makes use of users' personal information under law.

In our view, Article 24 does not explicitly prohibit enterprises from using user profiling for differentiated pricing (for example, offering cheaper prices or preferential subsidies to some new or inactive customers), but rather emphasizes that the use of such technologies should not lead to unfair results. That said, it is worth exploring further the precise boundary between differentiated sales strategies and "big data discrimination" that infringes upon personal rights and interests.

II Personalized marketing

Paragraph (2), above, applies primarily to "information push" (such as pushing various types of videos, articles, etc.) and "commercial marketing." Over the past year or so, regulatory enforcement has gradually come to focus on "targeted push" and "personalized display". The main points of concern have come to involve whether users are provided options that are not specific to their personal characteristics, the existence of mechanisms to deactivate or reject personalized options, and the actual effectiveness of those mechanisms[5]. When using users' personal information to carry out personalized display and targeted push, enterprises should respect the personal information subject's right to know (for example, through disclosure in privacy policies or by clearly identifying personalized and non-personalized content) and the right to choose (to ensure that users can refuse personalized content).

III Decisions that have a significant impact on personal rights and interests

Paragraph (3), above, emphasizes "decisions that have a significant impact on individual rights and interests". Based on EU legislation and enforcement experience, examples of significant impact on individual rights and interests include discriminatory treatment of individuals, refusal of transaction or employment opportunities, making reward and punishment decisions, and even making decisions with legal effect[6]. For such automated decision making, individuals have an "absolute right to know", i.e.,

[3] Article 13 (1) of the *Provisions on Administrative Penalties for Illegal Pricing (Revision Draft for Comment)*, an e-commerce platform operator sets different prices for the same goods or services under the same transaction conditions by using big data analysis, algorithms, and other technical means based on the characteristics of consumers or other business operators such as preferences and transaction habits, as well as factors other than cost or legitimate marketing strategies.

[4] According to Article 21 of *the Provisions on the Prohibition of Unfair Internet Competition (Draft for Comment)*, an operator shall not unreasonably provide different transaction information to a counterparty with the same transaction conditions, infringe upon the counterparty's right to know, right to choose and right to fair trade, and thereby disrupt the fair market trading order by collecting and analyzing the counterparty's transaction information, browsing the content and the number of times such information is viewed, the brand and value of the terminal devices used in the transaction, etc. Transaction information includes transaction history, willingness to pay, consumption habits, personal preferences, payment ability, dependence, credit status, etc.

[5] Recently, false deactivate buttons provided along with targeted push have also been included in the scope of special improvement campaign for the Internet industry launched by the Ministry of Industry and Information Technology "The Ministry of Industry and Information Technology launches special improvement campaign for the Internet industry". Please visit: http://mp.weixin.qq.com/s/GZkFr4DVxPPRvp0_RP8mAQ.

[6] For example, in the United States, algorithms are becoming more widely used in practice to assist judges in making parole

the right to ask the personal information handler to explain, and a "relative right of refusal", i.e., the right to refuse to the decision if the relevant decisions are made solely on automated decision making and without human intervention. The "absolute right to know" raises questions: (i) how should we understand the relationship between "require the personal information handler to explain" and the "right of interpretation" found in Article 48; and (ii) what is the required scope of the personal information handler's explanation. The latter may further address more complex issues such as the scope of algorithmic interpretation (e.g., whether it covers data disclosure and the interpretation of fundamental principles, accountability, fairness, safety and performance, and impact, etc.), and how to ensure the comprehensiveness of the interpretation.

Sensitive personal information processing: is separate consent the only legal basis?

Article 28 of the Final Draft designates the personal information of minors under the age of 14 as sensitive personal information, reiterating the classification of GB/T 35273-2020 *Information Security Technology – Personal Information Security Specification*. Personal information handlers can process sensitive personal information only if it is for a specific purpose and is sufficiently necessary and the handler undertakes stringent protection measures.

Notably, Article 29 of the Final Draft deletes the wording that "when processing sensitive personal information on the basis of personal consent" and stipulates only that "processing sensitive personal information requires the individual's **separate consent**, and if laws and administrative regulations provide that **written consent** is required for processing sensitive personal information, such provisions shall prevail."

There may be two ways to interpret this revision. On one hand, it can be interpreted that "separate consent" is the only legal basis for processing sensitive personal information. On the other hand, other legal bases for processing under Article 13 still apply, depending on the circumstances (subject to the conditions of specific purpose and sufficient necessary, and takes stringent protection measures). When processing sensitive personal information on the basis of consent, it is emphasized that the form of "consent" should meet the higher requirements.

We tend to think that the latter interpretation is more reasonable. This is mainly due to the broad definition of sensitive personal information under China's data law system and the PIPL's overall legislative mindset. Specifically, Articles 14 and 15 of the PIPL provide special requirements for processing personal information based on the individual's consent, such as the standard of consent (voluntary, explicit, informed), and the exclusive right when processing personal information based on consent (right of withdrawal). The other provisions in the text that refer to "consent" do not specifically restate "when processing is based on personal consent".

What "separate consent " means is another question that is worthy of discussion. This issue has not been clarified since the first draft of the PIPL. If we look at experiences abroad, the *General Data Protection Regulation* (the "**GDPR**") also distinguishes between "ordinary" consent and "explicit consent". Under the

decisions and providing reference for sentencing.

GDPR, consent should meet four conditions: "freely given", "specific", "informed" and "unambiguous"[7], which emphasizes that consent must be specific to the processing of data, rather than binding to the ability to use a product or service. For "explicit consent" required when processing special categories of personal data, in addition to the foregoing four conditions, emphasis is made that the consent must be made in an "explicit" fashion[8]. After the PIPL takes effect, enterprises can learn from the experience of GDPR to improve the "separate consent" mechanism.

Portability: extraterritorial experience to be localized

Chapter IV of the PIPL stipulates that individuals have the right to know, to decide, to restrict or refuse, to access and copy, to correct and complete, to delete, and to interpret. On the basis of the Second Reading Draft, the Final Draft of the PIPL creatively adds "if an individual requests to transfer his personal information to his designated personal information handler, and if the conditions specified by the national cyberspace administration department are met, the personal information handler shall provide the means for the transfer." This right draws on the well-known right to data portability under the GDPR. Data portability aims to solve the problem of "binding" users to large platforms, to increase users' mobility between different platforms of similar products, and to promote market competition while protecting users' right to choose.

The experience of GDPR can undoubtedly be used as a reference for how to refine the right to data portability in subsequent administrative rulemakings and for how enterprises can deal with this newly added "right to data portability". Article 20 of the GDPR grants data subjects the right to data portability. Under certain circumstances, data subjects have the right to obtain or instruct the controller to transfer to another controller the relevant personal data they have provided. Such personal data should be structured, commonly used, and machine-readable. According to the provisions of GDPR and related guidelines[9].

- **Exercise of the right is conditional**: that is, the data processing is realized by automation and is based on the data subject's consent or for the purpose of contract performance. In other words, a controller is not obligated to respond to data portability requests with respect to data processed under other legal bases (for example, where it is necessary to perform statutory duties or obligations).
- **Scope of exercise is limited**: the scope of portability under the GDPR is limited to the data "provided". EU regulators tend to interpret the scope of the "provided" broadly, by including personal data the controller obtains by observing user behavior, such as activity logs, website

[7] GDPR Preamble 32, "Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement."

[8] EDPB Guidelines for the Interpretation of Consents under GDPR (Guidelines 05/2020 on consent under Regulation 2016/679).

[9] 29th Working Group Guidelines for the Interpretation of Data Portability under the GDPR (Guidelines on the right to data portability under Regulation 2016/679, WP242 rev.01).

browsing records, but not data created by the controller through subsequent analysis of user data or user behavior, such as user profiling.

- **Data format requirements**: GDPR emphasizes that the data provided by the controller should be structured, commonly used, and machine readable. Where there is no common industry format, the guidelines encourage data controllers to use common open formats such as XML, JSON, CSV, and appropriate metadata.
- **Whether a fee may be charged**: in principle, fees are not allowed for data portability, but a reasonable fee can be charged when the data subject's request is unfounded or excessive, provided that the data subject should be immediately informed of the fees.
- **Whether a request can be rejected**: In principle, a controller cannot refuse to respond to a data subject's portability request on the grounds of technical or cost barriers. It is difficult to determine that the data subject's exercise request is beyond a reasonable limit simply because the cost of responding is too high. In addition, as industries currently process data in an automated manner, technical barriers are probably difficult to justify a rejection of the data subject's request.

At present, the Final Draft of the PIPL does not specify conditions for exercising the "right to data portability", but leaves it to the cyberspace administration department to formulate relevant rules. We believe that whether and how to implement the "right to data portability" in business practice will depend on the design of the top-level legislative system as well as exploration by market players. Only when the legislative system design is combined with industry practices can there be balance between the rights of the personal information subject and enterprise operating costs.

Mobile application-related liabilities and small personal information handlers: "more and less" in personal information protection regulation and law enforcement

Articles 61 and 62 of the Final Draft respectively provide for "more and less" in terms of the personal information protection duties of the departments implementing personal information protection, i.e., strengthening the supervision and administration of mobile applications while at the same time attempting to reduce the compliance obligations of small enterprises.

I "More" regulation: Articles 61 and 66 add application testing and evaluation as one of the duties of the personal information protection department and match the violations with penalties

Article 61 of the Final Draft of the PIPL expands the work duties of the personal information protection department by incorporating "organizing testing and evaluation of personal information protection practices within their application programs and publishing the testing and evaluation results". Accordingly, Article 66 specifically provides that "[w]here personal information is processed in violation of this Law or personal information is processed without fulfilling personal information protection duties in accordance with the provisions of this Law, the departments fulfilling personal information protection duties and responsibilities shall order correction, confiscate unlawful income, and order the provisional suspension or termination provision of the application programs unlawfully handling personal information…"

The above provisions provide a clearer higher-level legal basis for the supervision of apps and law enforcement by regulatory authorities in the past two years, and also lay a foundation for the final implementation of the *Interim Provisions on the Personal Information Protection of Mobile Internet Applications,* which has been released for public comments. It cannot be ignored that app testing and evaluation has gradually become an important means for supervising apps.

It is worth discussing whether the app testing and evaluation rules can replace the application of laws and whether the testing and evaluation results can replace legal judgments. We believe that app testing and evaluation is an efficient and convenient compliance tool, which has made significant contributions to improving the personal information protection levels in recent years. However, at the same time, we also call for the avoidance of rigid use of app testing and evaluation tools; instead, the reasonableness of the collection and use of personal information by APP should be specifically judged in light of specific scenarios.

II "Less" regulation: Article 62 stipulates that small personal information handlers will be subject to special personal information protection policies

The Second Reading Draft of the PIPL stipulates that the national cyberspace administration department will formulate special rules and standards for personal information protection in respect of processing of sensitive personal information and new technologies and applications such as facial recognition and artificial intelligence. On this basis, the Final Draft adds "small personal information handlers"[10].

Legislation abroad has long focused on how to avoid imposing too onerous a compliance burden on small enterprises, unreasonably increasing their operational costs, and avoiding curbing innovation. We are glad to see that the Final Draft responds to this question. We anticipate that future regulations may be in place to exempt small enterprises from certain personal information protection obligations.

Traces of this provision are found in laws abroad. For example, the California Consumer Privacy Act (the "**CCPA**") of the United States clarifies the scope of enterprises subject to the CCPA in terms of revenue, source of income, and amount of personal information, etc. Only those companies with annual revenue of $25 million, or processing 50,000 pieces of personal information, or 50% of annual revenue from the sale of personal information will be subject to the CCPA. Article 30 of the GDPR, in principle, exempts enterprises or organizations with fewer than 250 employees from the obligation to record personal data processing activities.

Personal litigation rights and public interest litigation: coping with personal information related litigation

Article 50 of the Final Draft adds "where personal information handlers reject individuals' requests to exercise their rights, individuals may file a lawsuit with a People's Court in accordance with law." This

[10] Article 62 of the PIPL stipulates that the national cyberspace administration department shall coordinate with the relevant authorities to promote the following personal information protection work in accordance with this law… (2) Formulate special rules and standards for personal information protection in respect of processing of sensitive personal information and new technologies and applications such as face recognition and artificial intelligence.

provision specifies that individuals have a series of litigation rights where personal information handlers deny the personal information subjects exercise of the right to know, to decide, to restrict or refuse, to access and copy, to data portability, to correct and complete, to delete, and to interpretation. According to the PIPL, which will enhance the types of civil litigation related to infringement of personal information rights.

In addition, Article 70 of the Final Draft also adds consumer organizations prescribed by law to those organizations that can file public interest lawsuits in matters relating to personal information infringement in accordance with the law.

These provisions related to litigation rights will no doubt provide more channels for lawsuits related to personal information infringement, in addition to the E-commerce Law and the Law on the Protection of Consumer Rights and Interests. When responding to supervision and law enforcement in the future, enterprises can expect to face increased pressure from personal information protection litigations from individuals, state organs, and consumer protection organizations, among others. It will be challenging for relevant enterprises to respond to such actions.

Summary and outlook

Prior to the PIPL, personal information protection was severely restricted due to an inadequate legal foundation, despite regulatory authorities having significantly strengthened the supervision and law enforcement of personal information protection in the past two years and the increased frequency of personal information-related litigation. This is reflected in the following situations.

- Limited scope of personal information protection. The previous personal information protection legislation has primarily consisted of the Cybersecurity Law and the Law on the Protection of Consumer Rights and Interests, which mainly target network services and consumer protection scenarios and cannot address the offline collection of personal information, especially employees' personal information protection scenarios.
- Relatively weak law enforcement. Although the law enforcement activities are frequent, most have focused on announcements, warnings, or small fines.
- Limited personal rights. The rights of personal information subjects have mainly focused on the right to know, to access, to correct, to delete, etc. Other personal information subject rights have lacked a basis at the legislative level and there has been insufficient protection of personal litigation rights.

The PIPL addresses these issues by providing systematic provisions on the compliance requirements for the following matters: all personal information processing throughout the data life cycle, the rights of personal information subjects, division of work and cooperation between regulatory authorities, personal litigation rights and public interest litigations, the effectiveness of extraterritorial application, and the cross-border transfer of personal information. Moreover, the PIPL will significantly increase the intensity of law enforcement and punishment. Going forward, we will undoubtedly see significant increases in the complexity of personal information protection, law enforcement efforts, and the frequency of lawsuits.

Notably, the PIPL will enter into force only two months following its promulgation, which reflects lawmakers' eagerness to have the PIPL come into effect as soon as possible. However, this short interval for preparation undoubtedly presents a significant challenge, both for enterprises and legal practitioners. In this regard, we suggest that enterprises in all industries attach great importance to personal information protection, comprehensively determine their personal information processing activities, and establish and improve personal rights protection mechanisms to avoid major compliance risk exposures. At the same time, we also hope that regulatory authorities will gradually promote enforcement of personal information protection provisions and provide time for enterprises and legal practitioners to study and adapt to the new law, so as to achieve an organic balance among personal information protection, healthy industry development, and stable market operations.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Kevin DUAN

Tel: +86 10 8516 4123
Email: kevin.duan@hankunlaw.com