提醒
ALERT

A Further Step Forward: China Releases Draft Personal Information Protection Law for Public Comment
更进一步：中国发布《个人信息保护法（草案）》征求公众意见

By Jenny Sheng(盛佳), Chunbin Xu(许春彬)

On October 21, 2020, the Standing Committee of the National People's Congress (NPC) of the People's Republic of China (PRC) released the draft PIP Law for public comment.

2020年10月21日，中华人民共和国（中国）人民代表大会常务委员会（人大常委会）发布《个人信息保护法（草案）》，并征求公众意见。

TAKEAWAYS

- With the big data industry rapidly growing in China and concerns about possible leaks and improper use of private data collected by various authorities and companies, the Draft PIP Law is a significant step to address the long-held concerns regarding personal data leaks and hacks.

  随着大数据行业在中国的快速发展，以及对各类政府机构和公司所采集的私人数据可能发生泄露和不当使用的担忧，《个人信息保护法（草案）》是作为解决长期以来对个人数据泄露和黑客行为的担忧所迈出的重要一步。

- Once promulgated, the Cybersecurity Law of the PRC, the Data Security Law of the PRC and this Draft PIP Law would constitute three fundamental laws of China that govern data privacy, data protections and cybersecurity.

  一旦《草案》正式颁布，《中华人民共和国网络安全法》、《中华人民共和国数据安全法》和《个人信息保护法》将构成中国治理数据隐私、数据保护和网络安全的三部基本法。

- The Draft PIP Law has extraterritorial effect, applying to overseas companies that do not have legal presence in the PRC but collect personal information directly from PRC individuals.

  《个人信息保护法（草案）》还具有域外效力，适用于在中国境内没有设立法律实体但直接向中国境内个人收集个人信息的境外公司。

10.21.20

The Personal Information Protection Law (Draft PIP Law) consists of eight chapters with 70 articles in total, covering a wide range of topics on protection of personal information, including (1) general principles; (2) rules of personal information processing; (3) rules of the cross-border transfer of personal information; (4) the rights of individuals; (5) obligations of data processors, (6) regulating authority; (7) legal liabilities; and (8) supplementary provisions.
《个人信息保护法（草案）》（"《草案》"）共八章 70 条，涵盖了有关个人信息保护的各类主题，包括（1）总则，（2）个人信息处理规则，（3）个人信息的跨境提供的规则，（4）个人在个人信息处理活动中的权利，（5）个人信息处理者的义务，（6）履行个人信息保护职责的部门，（7）法律责任，（8）附则。

Below is a summary of the key provisions of the Draft PIP Law.
以下是《草案》主要条款的概要。

Definitions of Personal Information and Sensitive Personal Information
个人信息和敏感个人信息的界定

Under the Draft PIP Law, "personal information" is defined as various types of information recorded in electronic or other forms relating to an identified or identifiable natural person, excluding information after anonymization. This is similar to the definitions under the General Data Protection Regulation (GDPR) of the European Union (EU) and California Consumer Privacy Act (CCPA).
《草案》将"个人信息"定义为"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"。这一定义与欧盟的《一般数据保护条例》（GDPR）和《加利福尼亚消费者隐私法案》（CCPA）的定义相似。

The Draft PIP Law gives a non-exhaustive list of sensitive data while the GDPR prohibits processing of defined special categories of personal data unless a lawful justification for processing applies. The term "sensitive personal information" under the Draft PIP Law is defined as "personal information, of which leakage or unlawful use may lead to discriminatory treatment or serious damage to personal or property safety, including race, ethnicity, religious beliefs, personal biometrics, medical health information, financial accounts, and personal whereabouts, etc.
《草案》就敏感个人信息进行了非穷尽性的列举，而 GDPR 则禁止处理特殊类别的个人数据，除非符合法定条件需要处理。《草案》将"敏感个人信息"定义为"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。"

Rules for Processing Personal Information
处理个人信息的规则

The Draft PIP Law sets forth general rules for processing personal information and special rules for processing sensitive personal information in Chapter 2. Most of these rules are consistent with those scattered among various existing laws and regulations.
《草案》在第二章中规定了处理个人信息的一般规则和处理敏感个人信息的特殊规则，大部分规则与分散在现行法律法规中的规则一致。

We address a few important rules for personal information processing below.
以下介绍处理个人信息的几项重要规则。

1) Individual Consent and Other Legal Basis for Processing
个人同意和其他处理个人信息的法律依据

Under the Draft PIP Law, the processing of personal information is not limited only to where consent has been obtained by the individual, as provided by the Cybersecurity Law. Under the Draft PIP Law, a personal information processor can process personal information on the ground of the following legal basis:
根据《草案》，个人信息的处理不仅限于《网络安全法》规定的取得个人同意的情况，符合下列情形之一的，个人信息处理者可以处理个人信息：

a. Processing personal information is necessary to enter into or perform a contract to which the individual is a party;
为订立或者履行个人作为一方当事人的合同所必需；

b. Processing personal information is necessary to perform legal duties or legal obligations;
为履行法定职责或者法定义务所必需；

c. Processing personal information is necessary to respond to public health emergency or to protect life, health and property safety of a natural person in an emergency;
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；

d. Processing personal information to a reasonable extent for the purpose of carrying out news reporting and public opinion monitoring for public interests;
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；

e. Other circumstances specified by laws and administrative regulations.
法律、行政法规规定的其他情形。

As compared to the GDPR, the Draft PIP Law spells out the need to process personal information in responding to public health emergency, which apparently addresses the continuing COVID-19 situation. However, the Draft PIP Law does not include "legitimate interests pursued by the controller or by a third party" under the GDPR as a legal basis for processing personal information.
与 GDPR 相比，《草案》表明了在应对公共卫生突发事件时处理个人信息的必要性，这显然是回应仍在持续发展的新冠病毒疫情。但是，《草案》并没有将 GDPR 规定的"控制者或第三方追求的合法利益"作为处理个人信息的法律依据。

2) Personal Information Processor
个人信息处理者

Unlike the GDPR, the Draft PIP Law does not distinguish between "data controller" and "data processor." The Draft PIP Law only specifies liability and compliance requirements on "personal information processor" that refers to organizations or individuals that independently determine the purpose, scope and methods of processing of personal information. The personal information processor defined in the Draft PIP Law is similar to the data controller under the GDPR.
不同于 GDPR，《草案》没有区分"数据控制者"和"数据处理者"。《草案》仅规定了"个人信息处理者"的责任和合规性要求，"个人信息处理者"被定义为"自主决定处理目的、处理方式的组织、个人"。《草案》中定义的"个人信息处理者"类似于 GDPR 下的"数据控制者"。

A personal information processor must not refuse to provide products or services on the grounds that an individual does not give consent to the processing of his or her personal information or withdraws his or her consent, except where the processing of personal information is essential for providing the products or services.
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。

Processors are obligated to adopt necessary measures to protect personal information, such as formulating internal management systems and operating procedures; categorizing personal information for management; adopting security technical measures (e.g., encryption and de-identification); conducting regular safety education and training; formulating and organizing the implementation of emergency plans for personal information security incidents.
个人信息处理者有义务采取必要措施保护个人信息，例如制定内部管理制度和操作规程；对个人信息实行分级分类管理；采取安全技术措施（如加密、去标识化）；定期进行安全教育和培训；制定并组织实施个人信息安全事件应急预案等。

A processor that processes personal information at a certain volume specified by the Cyberspace Administration of China (CAC) is required to designate a person specifically in charge of personal information protection whose name and contact information should be published and reported to the regulators. A processor is also required to conduct regular audits to ensure that its practice complies with the applicable laws and regulations.
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，该负责人的姓名、联系方式等应当公开，并报送给履行个人信息保护职责的部门。个人信息处理者应当定期对其个人信息处理活动是否符合法律、行政法规的规定进行审计。

3) Joint Data Processing and Data Processing by an Entrusted Third Party
共同处理个人信息和委托第三方处理个人信息

In case of joint processing, while the joint processors may agree on their respective contractual rights and obligations, the joint processors are jointly liable for any infringement on the rights and interests of an individual.
两个或者两个以上的个人信息处理者共同处理个人信息的，即使其约定了各自的权利和义务，如果侵害个人信息权益的，应依法承担连带责任。

Where a data processor entrusts a third party to process personal information, both parties shall execute an agreement that includes the means of processing, types of personal information, protective measures and rights and obligations of both parties. The processor should monitor the processing activities carried out by the third party. The third party is not allowed to further engage another party to process personal information without consent from the processor. After completion of performance of the contract or termination of entrustment, personal information shall be returned or deleted.
个人信息处理者委托第三方处理个人信息的，双方应当签署协议约定委托处理的目的、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。个人信息处理者应对受托方的个人信息处理活动进行监督。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。在合同履行完毕或者委托关系解除后，将个人信息返还个人信息处理者或者予以删除。

4) Processing of Sensitive Personal Information
处理敏感个人信息

The Draft PIP Law provides more restrictions on the processing of sensitive personal information. A personal information processor can only process sensitive personal information if it has specific purposes and such processing is sufficiently necessary, but the Draft PIP Law does not provide further interpretation of what constitutes "specific purposes" and "sufficiently necessary." Separate consent or written consent from the data subjects must be obtained before processing sensitive personal information.
《草案》对敏感个人信息的处理规定了更多限制。个人信息处理者只有具有"特定的目的"和"充分的必要性"，才能处理敏感个人信息。但《草案》并未进一步解释什么构成"特定的目的"和"充分的必要性"。处理敏感个人信息之前，应当取得个人的单独同意或书面同意。

Extraterritorial Application
域外适用

Multinational companies may be most interested in the contemplated extraterritorial jurisdiction of the Draft PIP Law, which might increase compliance risk for foreign companies that have operating subsidiaries in China or do not have a legal presence in China but provide products or services to Chinese individuals. The Draft PIP Law would apply to companies overseas:
跨国公司可能对《草案》中规定的域外管辖权最感兴趣，这一规定可能会增加在中国设有子公司或在中国没有设立法律实体但向中国境内个人提供产品或服务的外国公司的合规风险。《草案》将适用于下述境外公司：

1) that process personal information of individuals in China in order to provide products or services to them;
以向境内自然人提供产品或者服务为目的处理个人信息；

2) that analyze and assess the activities of individuals in China through the collection of personal information; or
为分析、评估境内自然人的行为而收集个人信息；或

3) for other purposes specified by laws and administrative regulations.
法律、行政法规规定的其他情形。

The above provision is similar to its counterpart under Article 3 of the GDPR, which applies, among other things, to the processing of personal data of data subjects in the EU by a controller or processor not established in EU.
上述规定类似于 GDPR 第 3 条中的相应规定，该规定适用于设立在欧盟境外的控制者或处理者对欧盟境内数据主体的个人数据所进行的处理。

In addition, the Draft PIP Law also resembles the GDPR provision and requires offshore processors that process personal information of individuals in the PRC to establish a designated office or appoint a representative in the PRC to be responsible for personal information protection in the PRC. Name and contact information of such office or representative should be submitted to the regulators.
此外，《草案》也与 GDPR 的规定相类似，要求中国境外处理中国境内个人信息的处理者在中国境内设立专门机构或指定代表，负责处理个人信息保护相关事务。该专门机构或代表的姓名和联系信息应报送履行个人信息保护职责的部门。

Cross-Border Information Transfer
跨境信息提供

A key issue about which many multinational companies with business in the PRC are concerned is the rules on cross-border information transfer.
许多在中国开展业务的跨国公司关注的一个重要问题是有关跨境信息提供的规则。

Article 38 of the Draft PIP Law provides that if a processor has business or other needs to transfer personal information to outside of the PRC, the processor must fulfil at least one of the following conditions:
《草案》第 38 条规定，个人信息处理者因业务等需要，确需向中国境外提供个人信息的，应当至少具备下列一项条件：

1) undergo a security assessment administered by the Cyberspace Administration of China (CAC) in accordance with Article 40 of the Draft PIP Law, which requires that operators of Critical Information Infrastructure (CII) and processors that transfer a certain volume of personal information (to be specified by CAC) must locally store personal information collected and generated in the PRC and must undergo a security assessment if cross-border transfer is necessary, unless such security assessment is not required by laws, administrative regulations and CAC rules.
依照该法第 40 条的规定通过国家网信部门组织的安全评估；第 40 条要求关键信息基础设施运营者 1 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将在中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，除非法律、行政法规和国家网信部门规定可以不进行安全评估。

2) obtain certification from a professional institution in accordance with the applicable CAC rules;
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；

3) enter into an agreement with the offshore recipient in which the agreement should specify the rights and obligations of both parties, and monitor and ensure that the offshore recipient can meet the protection standards provided in the Draft PIP Law; or
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《草案》规定的个人信息保护标准；或

4) other condition(s) to be specified by laws, administrative regulations or CAC rules.
法律、行政法规或者国家网信部门规定的其他条件。

It is likely that most processors would prefer to choose to meet item (3) since it does not involve a CAC security assessment or certification by a professional institution which may take time and incur additional cost. Item (3) is more likely to be chosen if the processor and the offshore recipient are affiliated companies. How this article will be passed in the final version of the law is an area to be closely watched.
大多数个人信息处理者可能更愿意选择满足上述第（3）项条件，因为其不涉及国家网信部门的安全评估或专业机构的认证，可以避免花费额外的时间和成本。在个人信息处理者与境外接收方是关联公司的情形下，更有可能选择满足上述第（3）项条件。最后通过的终稿中本条款将如何进行规定值得密切关注。

Even if a processor is allowed to transfer personal information to an offshore party, it is required to notify individuals of at least the following information: identity and contact information of the offshore recipient; purposes and means of processing; categories of personal information to be transferred; and the means to exercise rights under this law against the offshore recipient.
即使允许个人信息处理者将个人信息提供给境外接收方，其还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。

In addition, the processor must obtain a separate consent from everyone for such cross-border transfers.
此外，个人信息处理者还应就该等跨境信息提供取得个人的单独同意。

Similar to other recently published laws (e.g., Export Control Law) and regulations (e.g., Provisions on Unreliable Entity List), the Draft PIP Law also contemplates a "blacklist" to which the CAC has the power to designate offshore organizations or individuals conducting personal information processing activities that infringe rights and interests of PRC citizens relating to personal information, or endangering national security or public interest of the PRC. Processors will be prohibited or restricted from transferring personal information to such parties on the blacklist.
与其他最近发布的法律（如《出口管制法》）和法规（如《不可靠实体清单规定》）相似，《草案》也规定了"黑名单"制度，对于境外的组织、个人从事损害中国公民的个人信息权益，或者危害中国家安全、公共利益的个人信息处理活动的，国家网信部门有权将其列入该"黑名单"。个人信息处理者将被禁止或限制向黑名单上的组织或个人转移个人信息。

In addition, the Draft PIP Law provides that if any country or region imposes any prohibitive, restrictive or other similar measures in a discriminatory manner against the PRC with respect to personal information protection, the PRC may, based on actual circumstances, take corresponding measures against said country or region.
此外，《草案》还规定，任何国家和地区在个人信息保护方面对中国采取歧视性的禁止、限制或者其他类似措施的，中国可以根据实际情况对该国家或者该地区采取相应措施。

Legal Liability
法律责任

The Draft PIP Law imposes a fine of up to RMB1 million (approximately USD150,000) on the processor and up to RMB100,000 (approximately USD15,000) on the responsible personnel in case of a violation of the law. If the violation is considered serious, the fine may be up to RMB50 million (about USD7.5 million) or 5% of the processor's annual revenue for the prior year. While it is unclear whether the Draft PIP Law would combine the annual revenues of a group company in assessing fines on a processor, the proposed fine amount is significant.
《草案》对违反本法规定处理个人信息的，可处以最高100万元人民币（约合150,000美元）的罚款，对相关责任人员处以最高10万元人民币（约合15,000美元）的罚款。如果违法行为情节严重的，对于个人信息处理者可处以5,000万元人民币（约合750万美元）或相当于上一年度营业额5%的罚款。虽然尚不清楚《草案》是否会将个人信息处理者所在集团公司的年营业额来纳入评估罚款金额，但《草案》下拟议的罚款金额巨大。

Conclusions
总结

For multinational corporations that have subsidiaries in the PRC that process personal information and/or transfer personal information to the overseas' headquarters and affiliates, and for overseas organizations and individuals that collect information directly from individuals in the PRC for purposes specified in the Draft PIP Law, it is important to closely follow any developments of the Draft PIP Law. Multinational companies and domestic companies are recommended to start improving internal procedures and systems with reference to the Draft PIP Law. We expect that the NPC will review comments received from the public and publish a second draft for public comment or legislative review in the coming months. We will closely monitor further developments.
对于跨国公司在中国设立子公司处理个人信息和/或将个人信息转移到海外总部和关联公司，以及为《草案》规定目的直接向中国境内个人收集个人信息的境外组织和个人，密切关注《草案》的任何进展十分重要。我们建议跨国公司和国内公司根据《草案》开始优化内部规程和制度。我们预计人大常委会将在未来几个月审议公众的意见，并发布第二稿征询公众意见或进行立法审议。我们将密切关注未来的进展。