China's Personal Information Protection Law – How to Get Ready

Mark Schaub, Atticus Zhao

The growth of the digital economy has led governments around the world to seek to regulate cybersecurity and privacy of individuals. The digital economy has eroded national boundaries, accentuated possible risks to infrastructure and allows for personal information to be collected on a scale undreamt of and to be used in ways few understand.

China's authorities tackled cybersecurity with the PRC Cybersecurity Law (Cybersecurity Law) which came into effect on 1 June 2017. This law also touched upon privacy concerns and marked that regulating of the digital economy and cyberspace was a serious objective. On 1 September 2021, China Data Security Law came effect. The focus of this law is the protection and security of critical data in relation to national security and the public interest.

China's new Personal Information Protection Law (PIPL) which comes into effect on 1st November 2021 deals in a much more comprehensive manner with individual data. The Cybersecurity Law, the Data Security Law, PIPL and a plethora of other regulations need to be considered as a whole when international companies operate in or with China. However, as we explain in this article PIPL will likely cause much more concern for international businesses as 1) it is coming soon; 2) it applies much more broadly; 3) it establishes very legitimate rights for individuals vis a vis their personal data but such rights will need to be reflected in business processes; 4) the penalties have real teeth; and 5) one can expect very active enforcement due to a mix of motivated regulators and concerned individuals being empowered to take action.

In this article we seek to provide an overview as to how PIPL will hold companies accountable and also what measures we believe need to be taken.

What You Need to Know

1. The Big Issues

Time is of the Essence - On 1 November 2021, China's new *Personal Information Protection Law* (PIPL) comes into effect. Companies will therefore only have 2 months to analyze and comply with the new regime.

Who is in Charge of Enforcing PIPL? Will it be Enforced? The key regulator in charge of PIPL and its roll out is the Cyberspace Administration of China (CAC – also known as the State Internet Information Department). CAC which was only established in 2014 has been increasingly active in setting and enforcing PRC government policy in respect of data and cybersecurity. CAC has been very active in cracking down on tech companies that fail to follow data security regulations and often teaming up with SAMR (China's competition watchdog).

In addition to having a proactive and hands-on regulator in charge, PIPL implementation will also be buoyed by self-regulation on the part of China's big tech that wishes at all costs to avoid the ire of CAC (in particular consumer facing e-comm and sharing economy companies). It is worth noting that (Article 58) PIPL singles out the important internet platforms for several obligations including an obligation to stop providing services to products or service providers that are in serious breach. To ensure such gatekeepers have sound internal compliance system, the PIPL requires important internet platforms establish independent agency mainly composed of external members to supervise personal information protection.

However, perhaps the biggest issue for consumer facing companies is that the PIPL gives the right for the user to seek redress before the court if a data handler refuses to comply with a legitimate request. The power of the Chinese consumer should not be underestimated. In recent years, there are already cases brought by Chinese consumers before courts due to the services or products providers' harming of consumers' personal data. Chinese consumers are very keen to draw attention to corporate misbehavior to the courts, media or authorities.

Price of Non-Compliance is High – The PIPL has real teeth –serious breaches can result in fines of up to RMB 50 million or revenue confiscation of up to 5% of annual revenue and in most serious cases your business operations could be suspended or your company closed down. If your business relies upon APPs then such APPs may be taken down or suspended from digital platforms.

2. What does PIPL Change?

The main changes made by PIPL are:

Individuals will have more rights over the use of their data – including right to access, correct, restrict or have their data deleted. In addition, where consent is used as the legal basis for collecting and using personal data, individuals will have the right to withdraw their consent at any time. The bar for obtaining valid consent is set very high under PIPL (similar to current GDPR standard) as consent has to be informed, freely given (i.e. completely voluntary with no coercion) and explicit (i.e. the individual has to take an affirmative action to indicate their consent).

Data sharing/transfer – individuals will be provided far more detail as to who has access to their information, what they are doing with the data and which other parties are gaining access to such data.

Management Systems & Controls – Western companies that have grappled with GDPR roll out will be familiar with the requirements for putting privacy management systems in place. Companies will need to put systems in place to protect personal information in their custody.

Data localization – PIPL builds on the data localization requirements set out under the Cybersecurity Law for operators of critical information infrastructure (CIIO) and further requires personal data involving a large number of data subjects as specified by CAC to be located onshore an requires approvals to transfer offshore.

Learn more

We frequently publish thought pieces on China's business and legal sectors and trends. A selection of recent publications are below:

Videos:

- "China Art of Law" YouTube channel (all videos)
- Data & Cybersecurity Overview in China
- Cybersecurity and Data in China's autonomous sector

3. Questions to Consider

➢ Question 1: Will PIPL Effect My Company?

If you are doing business in or with China then it is highly likely to be yes.

It is also clear that the timeline to bring your businesses into compliance is ambitious. Despite the 1st November 2021 deadline it is likely that work will be needed for many months thereafter. Even in Europe with its 2 year transition deadline (not 2 months as for PIPL) few companies are likely to be fully compliant with their GDPR obligations – it may not even be possible. However, if your China business is already GDPR compliant then some adjustment would be required but most of the heavy lifting would already have been done. If no personal data management is in place in your China operations then a lot more work awaits.

In our opinion the companies that are most likely to be scrutinized under PIPL are:

China's tech giants – these are companies that manage and access enormous amounts of personal data. Recent events show that the Chinese authorities are keen to ensure these companies manage personal data responsibly.

Foreign Companies Reliant on China's Tech Giant – if you are reliant on the tech giants (i.e. ecomm sales; SaaS; gaming) then expect the tech giants to be the gate keepers – your non-compliance will be their non-compliance. And they really do not want to be non-compliant so vigorous vetting is expected. This may be an unexpected issue for foreign companies that have been operating offshore beyond the application of Chinese regulations. PIPL applies extraterritorially.

3. Questions to Consider (Cont.)

Consumer Facing Companies – China's consumers are increasingly active in holding companies to account. The growth in social media, use of internet and consumer protection laws means consumer complaints and lawsuits is an increasingly expensive and risky aspect of doing business in China for consumer brands.

Foreign companies Handling Mass Personal Data – if you have a sizeable China consumer facing business you may well face barriers to transfer personal data overseas. This may affect companies such as brands that analyze consumer information overseas for their loyalty programs or the like.

Foreign companies Handling Sensitive Personal Data – even if you are not dealing with mass levels of data you will face additional requirements if you are dealing with sensitive personal information. This could impact

- education – if you are collecting personal information of minors under age of 14;
- healthcare – if you are collecting or transferring health data or biometric data;
- fintech – if you deal with financial data;
- location tracking – this may be the one that leads to the most unforeseen problems as it could be problematic for many tech companies that rely on geo-mapping ranging from digital marketing; mapping; autonomous cars; ride hailing apps etc.

Using Biometric Personal Data – in addition a sensitive area is if you use or collect facial recognition, fingerprints, voiceprints or other biometric data from consumers or employees. This is a sensitive area for the government and individuals alike. As more and more APPs rely on biometrics it will be important to ensure individuals have a choice how to authenticate who they are and also how the collected data will be used.

3. Questions to Consider (Cont.)

- **Question 2: Will Chinese individuals have greater rights over their data? Will I need to change IT systems to accommodate? Is this fair?**

Yes.

PIPL will greatly enhance the rights of Chinese individuals over their personal information. These rights include the right to know and make decisions relating to their personal information; right to restrict or prohibit processing of their personal information; right to have copies of their personal information; right to the portability of their personal information; right to correct and delete their personal information; right to request organizations handling their personal data to explain their processing rules and right to withdraw consent.

In addition, Chinese consumers will be better protected from potential manipulation by big tech information pushing and digital marketing. In particular, consumers will have the right to refuse decisions being made automatically by algorithms based on collected data. In addition, personal information handlers will not be able to use data mining to differentiate offers between consumers (i.e. mostly charging different prices).

What does this mean for companies dealing with personal information from/in China?

IT systems will need to be able to do the following:

3. Questions to Consider (Cont.)

Where Consent is relied upon, obtain Informed and On-going Consent: handlers will need to inform consumers about who will be handling their data, purposes and methods, and their rights. In addition, specific consent will be required for sensitive personal information (i.e. including information such as on biometric identifiers, religious faith, medical data, financial status, and location tracking, as well as the personal information of minors under the age of 14) and for images (i.e. facial recognition, CCTV etc.). These requirements will give individuals greater control how their personal data is or is not used. It will also make it more difficult for covert data-mining being used for targeted marketing. Handlers dealing with sensitive personal information (most commonly this will be biometric data) will likely need pop up windows to ensure that explicit consent can be clearly shown. Companies will need to have privacy policies in place with individuals.

Make it convenient to withdraw consent: many have found that it is easy to click "OK" but challenging to find a way to say "Not OK" or "no longer OK". PIPL requires handlers to make it convenient and easy to let users withdraw consent. In addition, the handler cannot punish such a user by refusing to provide products or services unless the data was necessary to their provision. The Ministry of Industry and Information Technology (MIIT) has been very active in taking action in this respect against APPs. This is to stop covert data mining as APPs require access to personal information or microphone which is not relevant to their product or service.

Treat data sets differently: systems will need to differentiate between individuals that wish to exclude automated decision-making algorithms and those who find it convenient or do not care. Also IT systems will need to make it convenient for individuals to opt out of such algorithm based decision making (i.e. not just to use of their data). As PIPL requires information to only be used as required it may be wise to ensure systems have data segregation or masking options – this will allow personal information only to be viewed by those that need to.

Manage Data for Individuals:– Systems should facilitate access by individuals, allow for editing or deletion of personal information and provide copies upon request. Also as data should generally only be retained for the shortest time necessary the IT system should automatically delete data once the declared purpose has been achieved. There is precedent for this in that China's *E-commerce Law* (Article 24) grants users the right to deregister and delete their accounts and all information held by e-commerce operators, and also request copies of their personal information.

Allows for Data Portability: Individuals will be allowed to obtain, reuse and move their personal data for their own purposes. Transfers of data will need to comply with CAC requirements.

3. Questions to Consider (Cont.)

➢ Question 3: Do I Really Need to Put Anything Real in Place?

Companies that Handle Personal Data will need to Build a Privacy Management System

PIPL will require companies to do more than just theoretically comply with the law. PIPL does place an obligation on personal information handlers to put controls in place to avoid data leaks or hacks including:

- Internal security management systems and operating procedures;
- Implement categorical management of personal information;
- Use technical security measures such as encryption and de-identification;
- Determine reasonable operational authority for people handling personal information, periodic security education and training for relevant employees;
- Formulate and organize implementation of emergency plans for personal information security incidents;
- Regular security audits.

Personal information handlers will also need to make considered assessments of their personal information protection measures and make a record of how the data was handled when 1) handling sensitive personal information; 2) when using personal information for automated decision-making; 3) entrusting personal information to third parties or disclosing personal information; 4) providing personal information abroad; or 5) other personal information handling activities that will have a major impact on individuals' rights and interests.

In addition, companies handling personal information that meets the threshold that is to be specified by CAC will need to designate a person in charge of personal information (Article 52). Companies await with great interest what threshold CAC will specify with guesses ranging from 100,000 data sets or people (based on mobile date regulations) to 1,000,000 based on this being the CAC's requirement that would trigger a cybersecurity review of a Chinese centric company seeking an overseas listing.

If your company is based overseas then you will need to find a designated representative or establish an organization within China – this may be a WFOE, rep office or other trusted individual. This is similar to the requirement for overseas cosmetics companies appointing a local representative. This has been a headache for those who do not have on the ground Chinese operations. Given the potential liability under PIPL it is difficult to imagine that law firms or accounting firms will be lining up to act in this regard.

3. Questions to Consider (Cont.)

Companies will need to consider how they deal with Employee Data

Most of the focus by Western companies will be on how to deal with consumer personal data (and in some cases suppliers or partners). The other group which will very likely affect every foreign invested enterprise (FIE) in China is how to deal with employee personal data.

The main challenges in respect for employee data will be as follows:

Data exports – many FIEs will collect sensitive personal data from their China based employees (e.g. HR and payroll data such as name, address, email address, salary, nationality, ethnicity, gender, etc.) and then transfer such data overseas. It will be necessary to obtain explicit consents from employees and follow the cross-border transfer requirements..

Third Party Processing – in addition many FIEs rely on payroll by third parties in China and sometimes offshore. Also many have HR data included in a global IT system – again often operated by a third party vendor. These arrangements will need to be scrutinized.

Measures to be Taken for Employees - Most FIEs will need to update their standard employment contracts or employee handbook to require express consent for transferring employee personal data abroad as well as issuing an Employee Privacy Policy. Such new policies will likely be treated as “regulations and rules” of the employer and thus would need to be provided to all employees for discussion beforehand.

Companies will need to look at their Third Party Vendor Arrangements

PIPL sets requirements for processing activities by third parties including joint processing and third-party processing. Accordingly, companies will need to have contracts in place with such vendors (many do not) and also inform individuals as to the identity of the third party data processor and that they will comply with the ambit of the given consent. Any changes to the consent would require additional explicit consent by the affected individuals. This will be an issue for companies using third party HR (payroll), outsourced marketing or CRM systems.

3. Questions to Consider (Cont.)

➢ Question 4: Will it be Possible to transfer PI Cross-border?

Data localization and cross-border data flow have long been a focus of national data protection legislation of various countries.

The PIPL requires the cross-border exporter adequately inform individuals and obtain their specific consent before their data is sent overseas. In addition, the PIPL expands the data localization and cross-border rules set under the Cybersecurity Law beyond CIIOs to also include "personal information handlers (“Mass Handlers”) who process personal information up to the number regulated by CAC”. PIPL requires CIIOs and Mass Handlers pass a CAC security assessment before they can transfer personal information offshore. The threshold of number of individuals involved is still to be specified by the CAC but as mentioned above likely to be somewhere between 100,000 and 1,000,000 pieces of data.

For enterprises that are not considered CIIO or Mass Handlers, PIPL provides a variety of data export pathways for exporting data provided they meet one of the requirements from "satisfying the security assessment organized by the Cyberspace Administration (exceptions exist)"; "being certified by the professional organization designated by CAC "; or "enter into a contract with the overseas recipient under the standard contract formulated by the CAC, specifying the rights and obligations of both parties" or other conditions prescribed by laws. This does show PIPL takes into account commercial needs and facilitates data export by low risk data handlers.

Thus, Mass Handlers and CIIOs will need to localize storage of locally collected or generated data in China and also pass a security assessment of the CAC before they can transfer personal information offshore. Details as to mass handling thresholds, security assessment and precedent contract clauses will likely be fleshed out in implementing regulations.

3. Questions to Consider (Cont.)

➢ Question 5: Does PIPL apply if my business is operating offshore?

Many international businesses operate into China from overseas on the belief (mostly right) that Chinese laws do not apply. PIPL is a rare example of a PRC law that explicitly has extraterritorial effect (PRC Cybersecurity Law was another example). Offshore companies processing personal information of natural persons in China will be caught within the ambit of PIPL under the following circumstances:

- the offshore processing of data is for the purpose of providing products or services to natural persons within China;
- the offshore processing of data is to analyse/evaluate the behaviour of natural persons in China; or
- other cases as specified by laws and regulations.

As outlined above any offshore business falling within the PIPL ambit will need to designate a representative or organization in China to handle personal information protection issues. Digital companies such as offshore education websites and SaaS businesses will be most affected but also companies engaging in cross border ecommerce will need to comply with the requirements.

Next Steps

It is safe to say no-one has all the answers at present and much will depend upon future implementing regulations and policies to be issued by CAC. However, clearly PIPL provides sufficient guidance for companies to address as soon as possible privacy issues in respect of consumers, employees, suppliers, partners etc. If you have provided GDPR type protection to European stakeholders why not Chinese stakeholders? Not having the full picture will not be a good excuse for not starting to address obvious issues.

We have prepared a self-administered checklist of potential issues to consider when reviewing your readiness level. Such list is being constantly updated. If it is of interest please let us know and we can send you the latest version.

The other issue is that almost every company will have its own bespoke issues. We welcome interacting with clients on this issue and are happy to schedule a free of cost initial Teams session to discuss your concerns and answer initial queries. Such meeting can be scheduled with Shawn Hu of our Shanghai office. Please contact him on shawn.hu@cn.kwm.com

Awards and recognition

King & Wood Mallesons, with its strong foundation and ever-progressive practice capacity, has been a leader in the industry. King & Wood Mallesons has received hundreds of international and regional awards from internationally authoritative legal rating agencies and business and legal media in recent years.

- No. 1 in Acritas' Asia Pacific Law Firm Brand Index
  Acritas, 2020
- No. 11 in Acritas' Global Elite Law Firm Brand Index
  Acritas, 2021
- Most Innovative Law Firm in the Asia-Pacific
  Financial Times, 2021
- China (PRC) Law Firm of the Year
  Chambers Asia-Pacific Award Asia, 2020
- Regional Law Firm of the Year, Most Innovative China Law Firm of the Year
  IFLR Asia Awards, 2021
- China Law Firm of the Year
  ALB China Law Awards, 2021
- Innovation in Strategy and Changing Behaviours
  Financial Times 2019
- Law Firm of the Year and Best Overall Law Firms
  China Business Law Journal, 2018
- Asia-Pacific Innovative Lawyers Awards 2017: 'Innovation in Legal Expertise' and 'Innovation in the Business of Law'
  Financial Times, 2017
- Most Innovative Law Firm in the Asia-Pacific
  Financial Times, 2014-2015
- North Asia Firm of the Year
  asialaw Profiles, 2017
- Firm of the Year-China
  Who's Who Legal, 2016

"THE FIRM WORKS TOGETHER WITH CLIENTS TO SHAPE A NEW WORLD FOR THEIR BUSINESS, CREATING REAL VALUE BY COMBINING ENTREPRENEURIAL SPIRIT WITH INTELLECTUAL RIGOUR AND DEEP LOCAL KNOWLEDGE, TO PROVIDE QUALITY LEGAL SOLUTIONS THAT ARE INNOVATIVE AND OFTEN GROUND BREAKING."

Chambers Asia Pacific

金杜律师事务所
KING&WOOD
MALLESONS

A little bit about us

MARK SCHAUB

Managing Partner
Shanghai, London, Frankfurt
T +44 20 7550 1564 (UK)
mark.schaub@eu.kwm.com

ATTICUS ZHAO

Partner
Shanghai
T +86 21 2412 6154
atticus.zhao@cn.kwm.com

MARK FU

Partner
Shanghai
T +86 21 2412 6241
fuguangrui@cn.kwm.com

SANA DUNCAN

Of Counsel
London, United Kingdom
T +44 (0)20 7550 1678
sana.duncan@eu.kwm.com

SHAWN HU

Foreign Legal Consultant
Shanghai
T +86 21 2412 6370
shawn.hu@cn.kwm.com

EFFIE LIU

Senior Associate
Shanghai
T +86 21 2412 6205
liuguannan@cn.kwm.com

TOM SHI

Associate
Shanghai
T +86 21 2412 6138
shiwei3@cn.kwm.com

MICHELLE YE

Associate
London
T +44 20 7550 1577
michelle.ye@eu.kwm.com