PRIVACYRULES

# DOING BUSINESS IN AND FROM CHINA,
## WHAT CHANGES WITH THE NEW CHINESE PRIVACY LAW

## THE RECORDING OF THE WEBINAR IS AVAILABLE HERE

# SPEAKERS

**JIHONG CHEN FROM ZHONG LUN LAW FIRM - CHINA**

CONTACT JIHONG CHEN

**CHIARA AGOSTINI FROM RP LEGAL & TAX LAW FIRM - ITALY**

CONTACT CHIARA AGOSTINI

**SHARON LUO FROM THE INTERNATIONAL CYBERSECURITY COMPANY WIZLYNX GROUP – CHINA BRANCH**

CONTACT SHARON LUO

**LUCA EGITTO FROM RP LEGAL & TAX LAW FIRM - ITALY**

CONTACT LUCA EGITTO

# EXECUTIVE SUMMARY

On November 24, PrivacyRules hosted a webinar to delve into key implications for businesses of the new Chinese privacy law - the Personal Information Protection Law (PIPL) - that came into force on November 1, 2021.

**Jihong Chen** from the Chinese law firm Zhong Lun opened the event by addressing the most relevant elements of the PIPL for foreign companies operating in China. Next, the experts **Chiara Agostini** and **Luca Egitto** from the Italian law firm RP Legal & Tax presented the differences and similarities between the European General Data Protection Regulation (GDPR) and the PIPL. To conclude, Sharon Luo the Managing Director of the China branch of the international cybersecurity company Wizlynx Group focused on the most relevant cybersecurity aspects that companies have to implement and deploy in order to comply with the PIPL.

This report summarises core insights and takeaways from the panelists, to guide clients towards compliance with the new law and the broader Chinese framework concerning Personal Information (PI) processors. We strongly advise national and foreign companies to take a glance at this report and follow the recording of the webinar available at www.privacyrules.com, especially considering the high sanctions that could be imposed against those who do not take appropriate steps to ensure legal and cybersecurity compliance.

Among the main novelties of the PIPL are its extraterritorial application and the special focus it poses on cross-border data transfers. Concerning who are requested to abide by it, companies and PI processors of data of persons in China must apply the provisions of the PIPL even when their headquarters are not located within Chinese territory. To establish compliance, these must have local representatives and expert personnel including both specialized agencies and adequately trained in-house personnel.

A clear outcome of this webinar is that the PIPL is more strict when compared with the GDPR when it comes to regulatory preventive and corrective assessments and processes.

The implementation of cybersecurity services and solutions is essential to effectively fulfill PIPL compliance requirements, therefore it is highly recommended to have support and guidance from specialised legal and cybersecurity experts for conducting business in China.



# WALKING FOREIGN COMPANIES THROUGH THE COMPLIANCE CHANGES OF THE NEW CHINESE PRIVACY LAW

*by Jihong Chen from Zhong Lun law firm.*

Mr. Chen opened the discussion by highlighting the scope, context, and the most important legal elements of the PIPL, structuring his presentation to provide guidance to foreign companies operating or planning to operate in China. The expert outlined that the PIPL has complemented the "Three Pillars'' of China's data protection legal framework, together with the Cyberspace Law and the Data Protection Law.

The new privacy law seeks to regulate the way in which processors obtain and manage Personal Information (PI) of individuals in China, whether the processors are within its territory or not (Art. 1- 3).

Concerning its extraterritorial nature, there are two specific situations in which this law has such extensive application:

- to companies and entities providing services or products to natural persons within China
- when companies and entities analyse or assess their conduct (Art.3)

The PIPL indicates seven main bases which processors must comply with:
personal consent

1. necessity for the execution of a contract or human resources management
2. necessity to perform legal duties or legal obligations
3. necessity to respond to public health emergencies
4. legitimate public interest
5. legally disclosed personal information, and
6. other circumstances stipulated by laws or administrative regulations.

Additionally, the PIPL addresses nine main principles:

1. Lawfulness
2. legality
3. necessity
4. sincerity
5. purpose limitation
6. data minimization
7. transparency
8. accuracy, and
9. Accountability

The new law also safeguards the individual rights of people of, among others, knowing, deciding, restricting, correcting, and deleting their PI (Art. 13).

In order to ensure compliance with the PIPL, processors must have personnel responsible for the PI as well as local representatives. Furthermore, processors must establish an internal managing system and operational rules (Art.51.1), regular reviews and audits (Art. 54), PI protection impact assessments (Art.55), and, in addition to other security requirements, they must warrant classification rules on PI, encryption and de-identification measures, access control and regular training and PI incident response plans.

The PIPL prescribes several administrative penalties (even higher than the GDPR ones), from economic and corrective actions, confiscation, warnings, suspension of service, to the prohibition to exercise activities related to data protection and PI, public interest class action lawsuits and reporting to credit archives up to their disclosure to the public (Chapter VII).
The PIPL vs. GDPR:

While the two regulations present several similarities, there are also important differences. Some of the key terms are defined differently in the two regulations: the PIPL refers to "personal information", "processors'' and "sensitive personal information" while the GDPR refers to "personal data", "controllers" and "special categories of personal data".

Both the PIPL and the GDPR have as a requirement for processing personal information: human resources management and contract processing. However, the PIPL adds as a requirement that the PI has been disclosed by the data subject or by lawful means (Art. 13). Similarly, the PIPL is more directive when it comes to compliance with assessments and certifications, such as the certification of IP protection and the assessment of cross-border transfer mechanisms of the Cyberspace Administration of China (CAC) (Art. 38). Finally, another important difference between the two laws is that "legitimate interest" is not a concept provided by the PIPL.

Key take-aways for foreign companies:
The PIPL applies to foreign companies when their purpose is to provide services or products to natural persons within China, or for the analysis and evaluation of the activities of natural persons within China (Art.3).

Separate consent is required when the processor:

1. provides PI to other processors (Art. 23)
2. publicly discloses PI (Art. 25)
3. collects images and personal identification through public recording equipment for the purpose of preserving public security (Art. 26)
4. processes sensitive PI (Art. 29), and
5. when it transfers PI outside China (Art. 39)

A Personal Information Protection Impact Assessment (PIA) is required when processing sensitive information; making automated decisions; entrusting, providing, publicizing PI to others; and, other activities that may impact personal rights (Art. 55). The PIA must include the lawfulness, legitimacy, and necessity of the PI processing, the impact on personal rights, interest and security risks, as well as the lawfulness, effectiveness and proportionality with the risks (Art. 55).

And finally, the PIPL prescribes that personal information must be stored inside the territory of People's Republic of China, considering the conditions set out in its Article 40.

# THE GDPR MINDSET AND ITS POSITIVE IMPACT WHEN ACCESSING THE NEW CHINESE PRIVACY LAWS

*by Chiara Agostini and Luca Egitto from RP Legal & Tax law firm.*


Ms. Agostini and Mr. Egitto discussed the PIPL from the European perspective, outlining key similarities and differences between the European GDPR and the Chinese PIPL. Both regions have companies and entities sharing different commercial and service relationships and in general, are handling information and personal data of respective subjects.

Regarding the territorial scope, the GDPR focuses on the activities carried out within the European Union while the PIPL focuses on the processing of personal data within the territory of China. When it comes to profiling, both the GDPR and the PIPL apply to processing of personal data of subjects who are physically in their respective borders, regardless of the place in which the data controller is located or the data processing is carried out (Art. 3).

Controllers - processors in the PIPL - outside the EU borders shall designate a representative to manage EU data. Similarly, data originating from China require the designation of a representative or the establishment of a special agency within this territory (Art. 53). Notably, there is an exception under the GDPR: a representative is not needed when the processing of data is occasional and no special categories of data are involved.

The GDPR requires the appointment of a Data Protection Officer (DPO) with particular skills and the indication of its contact information accessible to data subjects through the controller's privacy notice and notified to the competent authority. The PIPL does not have any specific role requirement for the person in charge of personal information protection within a given company or entity, nevertheless, this person is still required to disclose its contact information – similarly to the GDPR – and is burdened by personal legal liability, unlike in the GDPR (Art. 9).

The legal bases that apply to the processing of common personal data under the GDPR are similar to the ones of the PIPL but, in the new legislation, they apply to the processing of any kind of data, such as health records and political opinions. The EU law has a legal basis that allows processing for legitimate interest by the data controller, while the Chinese law does not. In addition, the PIPL allows the processing of personal data legally disclosed by individuals while the GDPR allows it only for special data categories (Art. 9).

Both laws don't allow free international data transfers. Specific conditions are required to be met for such transfers: the PIPL provides a higher level of involvement by public authorities, especially in cases of cross-border data transfers (Chapter III) whereas the GDPR focuses more on the accountability principle.

Moreover, according to the PIPL, international transfers require the data subjects' separate consent (Art. 39) and cybersecurity and data protection impact assessments, while the GDPR has no such specific obligations.

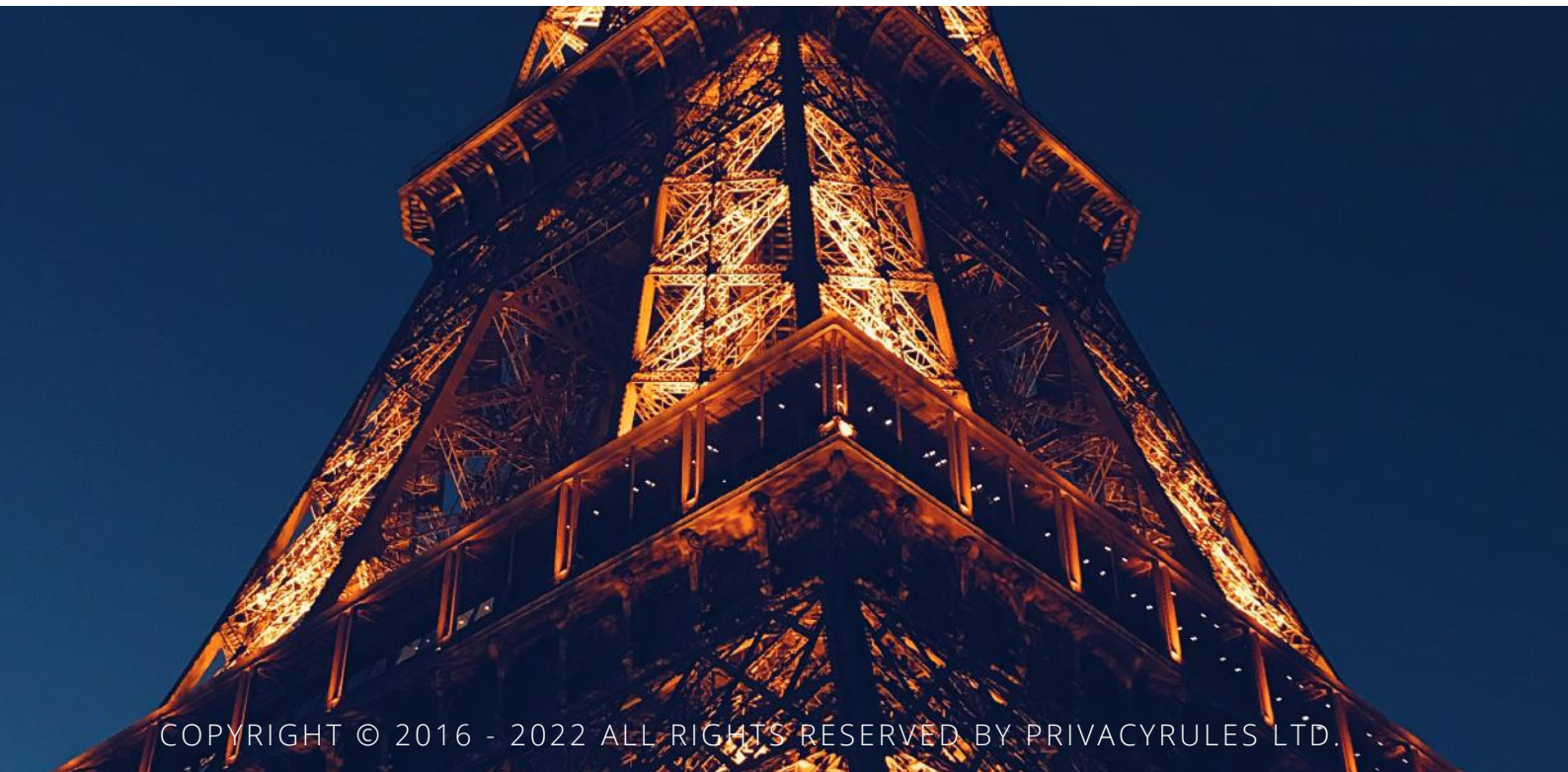
Under the GDPR, security measures to be adopted by the data controller are based on the accountability principle whereas under the PIPL, the types of security measures are foreseen by the law itself.

European companies shall assess the PIPL impact, allocate special budgets and monitor developments of the PIPL application by local authorities. Companies that already have a high degree of compliance with the GDPR will have a significant competitive advantage over those that do not possess the same level of compliance.


Comparative chart on key elements of the PIPL and the GDPR (as of December 2021):

| Criteria | Similarity (goes in overlap) | Difference (separate circle part) | |
|---|---|---|---|
| | **GDPR and PIPL** | **GDPR** | **PIPL** |
| **Key definition** | .Privacy and protection law. | Personal 'data'<br>'Controllers'<br>"Special categories of personal data" | Personal 'Information'<br>'Processor'<br>'Sensitive Information' |
| **Legal Bases**<br>(Requirements to allow data processing | 1. Consent.<br>2. Conclusion and performance of a contract.<br>3. Health emergencies.<br>4. For statutory duties.<br>5. Public interest. | Legitimate Interest. | Personal data disclosed legally by individuals usable for all categories of data. |
| **Scope** | Territorial scope<br>Profiling scope. | | |
| **Subjects to be Appointed** | 1. Designate a representative.<br>2. DPO/Person in charge of personal information protection: disclosure of information contact to the competent authority. | 1. Exception : occasional and no special categories of data involved.<br>2. Data Protection Officer with technical requirements.<br>No personal legal liability. | 1. Representative could be a special agency or a Representative.<br>2. Person in change with no specific requirements.<br>Personal legal liability. |

| Criteria | Similarity (goes in overlap) | Difference (separate circle part) | |
|---|---|---|---|
| | **GDPR and PIPL** | **GDPR** | **PIPL** |
| **International Transfers** | Do not allow free data transfer outside respective borders.<br><br>Privacy notice. | No obligation of data protection impact assessment.<br><br>Emphasis on accountability principle. | PI protection impact assessment is required.<br><br>Separate consent of data subjects.<br><br>Public authorities are higher involved. |
| **Security measures** | Both establish legal and technical measures. | Assessments and measures are highly recommended.<br>Emphasis on accountability principle. | Assessments and measures are mandatory. |





# CYBERSECURITY PERSPECTIVE ON HOW TO COMPLY WITH THE NEW LAW

*by Sharon Luo from the international cybersecurity company Wizlynx Group – China branch.*

Ms. Luo underlined that the PIPL was also established to uplift information security and data protection services in various organizations to a higher level. From a cybersecurity perspective, several services of every kind of company and entity possessing and processing PI need to be updated and comply with the new law. The law outlines the compliance processes that are considered to be beneficial for companies based in China as well as for any company that possesses PI of Chinese individuals; this serves as a guideline to modify individual policies and services, in order to become effectively compliant with the PIPL.

A first process consists of analysing the cybersecurity compliance requirements of the PIPL and identifying the related methodologies that are needed to align with what is prescribed by the main 5 articles of the PIPL making specific reference to cybersecurity: namely, articles 51, 54, 56, 57, and 59.

A wise action plan to comply with the PIPL from the cybersecurity perspective can be divided into 4 main components:

- PIPL risk and Compliance Assessment (Art.54, 56)
- Information Security Management System (Art. 51, 57)
- Penetration Testing with Remediation (Art.57, 59)
- Social Engineering with Training (Art.59)

There are three possible cybersecurity solutions that can help clients and customers to comply with the PIPL. Each process is conducted to ensure that all the requirements have been met and that they also cover external parties.

Firstly, cybersecurity solutions that support clients with asset and data inventory and classification, risk assessments and management, PIPL audits and compliance assessments, information security management system (ISMS) implementation, policies and procedures and roles, and remediation action tracking (solutions provided for instance by the "360inControl" Wizlynx service).

Secondly, phishing assessments and training platforms (like the ones provided by the Wizlynx "Phishlynx" service) offer essential training features such as realistic simulation, dashboard & reporting, build-in awareness training, and professional services. Often the weakest link in cybersecurity is human-related, hence these services are created to focus on how to remediate vulnerabilities linked to human errors by presenting various phishing methods, and thwart the attempts of bad actors to get access by using valid credentials acquired through social engineering techniques.

The third cybersecurity solution consists of dedicated "Offensive Cyber Security Assessments". This methodology simulates real cyber-attacks and aims at identifying system vulnerabilities in a target company and the respective technical safeguards that need to be adopted to mitigate threats to companies' data.

In conclusion, the implementation of the new law requires a comprehensive approach that includes cybersecurity solutions planned and executed in cooperation with well-prepared cybersecurity specialists already abiding with best practices such as NIST, ISO/IEC 27000 family of standards, and others.

## DRAFTED BY:

Adriana López, Baramee Chamnankij, and Priyanka Kaushik – interns at the PrivacyRules Cybersecurity Partnership Program

## CLEARED BY:

Andrea Chmieliński Bigazzi, CEO of PrivacyRules

**Last revised: 23 December 2021**