tsaaro

secuvy | ai

WHITEPAPER

CHINA'S PERSONAL INFORMATION PROTECTION LAW

Your Guide to China's Personal Information Protection Law.

INTRODUCTION

The Personal Information Protection Law (hereinafter referred to as “PIPL”), of the People’s Republic of China was passed on the 20th of August, 2021, which would come into force on the 1st of November, 2021. This is China’s initial comprehensive personal data protection framework, that extensively regulates the processing and transfer of personal information of the natural persons of China. This special law introduces stringent provisions for protecting the personal information rights and interests, processing of personal information and promoting the reasonable use of personal information.

PROBLEM

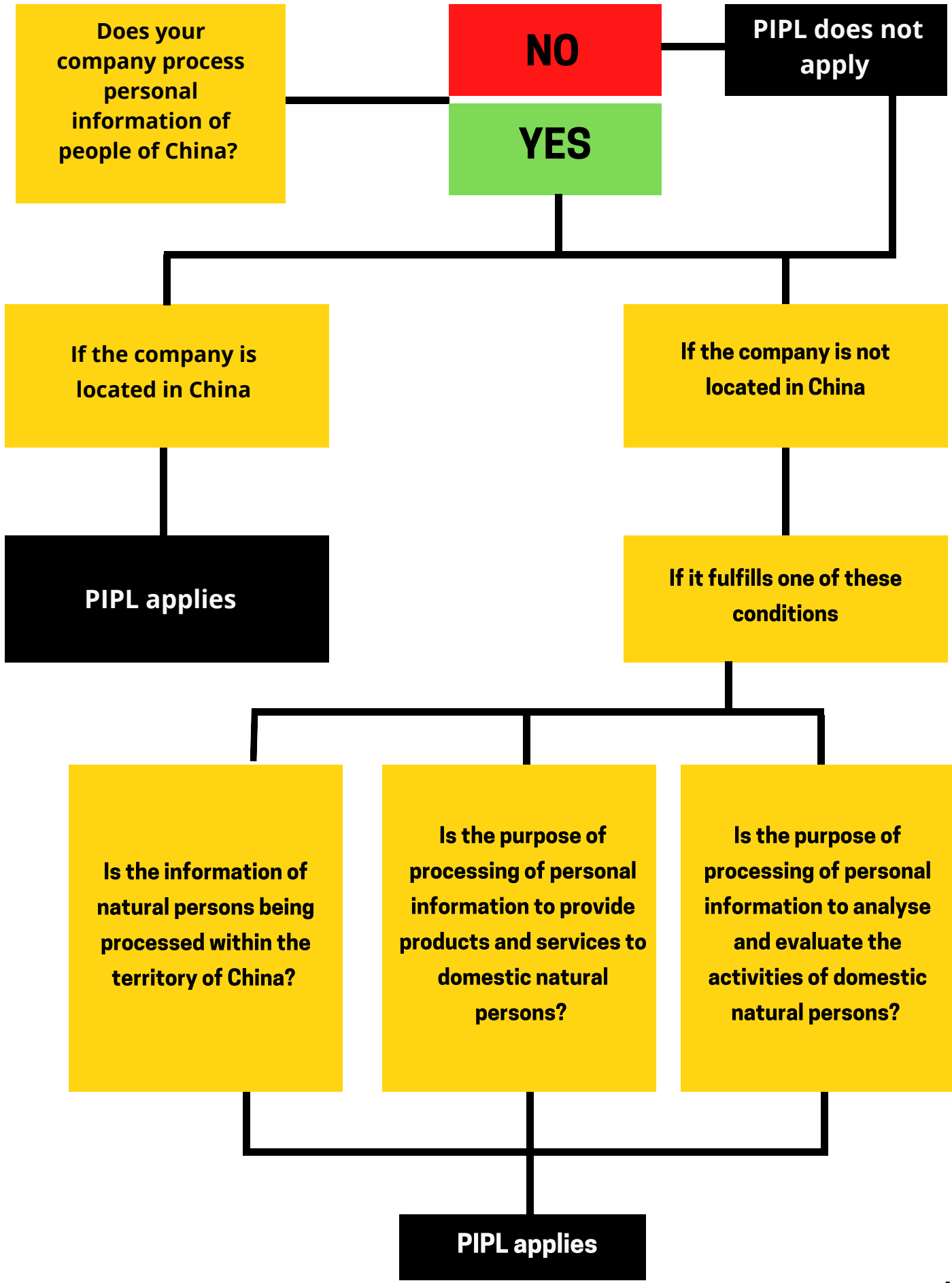
With the PIPL set to take effect in about a month, organizations and businesses that engage in core activities involving data will be compelled to comply with its prescribed regulations. This could potentially attract complexity, with the limited time-period between the passing of the law and the law coming to effect.

LEGAL PROVISIONS

The PIPL has been formulated after a revision, which categorically lays out detailed rules for processing personal information and sensitive personal information. It also stipulates obligations entrusted to personal information handlers, restrictions on personal data transfer, strict penalties, and legal liability. The **key provisions of PIPL** are:

- Applicability of PIPL
- General Principles of Processing Personal Information
- Rules for Processing Personal Information
- Rules for Processing Sensitive Personal Information
- Special Provisions on Processing Personal Information by State Organs
- Rights of Data Subjects
- Cross-Border Provision of Personal Information
- Legal Liability

APPLICABILITY OF PIPL



GENERAL PROVISIONS OF PIPL

INTERPRETATION OF KEY PHRASES

Personal Information: Information pertaining to the identification of a natural person. This information may be recorded through electronic or any other means excluding anonymous information.

Personal Information Handler: An organization or individual that determines the purpose and means of processing personal information.

Processing: Collection, storage, processing, transmission, provision, publication, and erasure of the personal information.

Sensitive Personal Information: Personal Information that could infringe the personal dignity of a natural person upon being leaked or illegally used. This is inclusive of information such as bio-metrics, religious belief, specific identities, medical health, financial accounts, whereabouts, and the personal information of minors under the age of 14.

GENERAL PRINCIPLES OF PROCESSING

- Legality, legitimacy, necessity, good faith, transparency and openness.
- Prohibition on the processing, by misleading, fraud or coercion.
- Purpose Limitation wherein data collected for a particular purpose should not be used for another purpose.
- Maintaining the accuracy and the quality of the personal information.
- Restrictions on processing, collecting, using, transmitting, trading personal information illegally.
- Restrictions on provisions or disclosure, or processing that could endanger the national security or public interest.

RULES FOR PROCESSING PERSONAL INFORMATION

1. The consent provided by the individual must be voluntary, explicit and given in the knowledge of the individual. The consent must be re-obtained in case of any change in the purpose or method of processing.

2. Prior to processing, the handler is required to provide his name and contact information, the purpose and method of processing, retention periods to the data subjects.

3. The handler can process personal information without the consent of the individuals in the interests of the life, health and property safety of natural persons. The requirement of confidentiality and non-disclosure of the personal information processed by the handler is subject to certain exceptions of laws or regulations.

4. In case the handler entrusts any other handler to process the personal information of the individuals, the entrusted party is under the obligation of the contractually validated purpose, duration, and method of entrusted processing, type and protection measures of personal information and the rights and obligations of both parties.

5. If the personal information is being transferred by its handler to a third party, the individual concerned must be duly informed of the name and contact information of the third party, purpose and method of processing and type of personal information, and must obtain separate consent.

6. The period of retention of the personal information processed must be minimum in consonance to the purposes and objectives of the processing of such personal information. This is exempted in cases where the law or administrative regulations provide otherwise.

RULES FOR PROCESSING SENSITIVE PERSONAL INFORMATION (SPI)

1. Information handlers may only process sensitive personal information for specific purposes and when sufficiently necessary. The law includes a prohibition for handlers to disclose the PI they are processing, unless they obtain specific consent.

2. Prior to the personal information being processed, consent must be obtained from data subjects, and has to be informed, explicit, voluntary and individuals are also vested with the right to rescind their consent. New consent must be obtained in case the purpose or the methods of processing changes or if shared with any third-parties.

RIGHTS OF DATA SUBJECTS

RIGHT TO BE INFORMED: The mandatory information to be provided before processing includes: identity of the personal information handler and contact details; purposes for processing; means of processing; types of personal information to be processed; retention period; how individual's rights may be exercised.

DECEASED'S DATA SUBJECT RIGHTS: A close relative may, for his or her own lawful and proper interest, request sight, copy, amendment and erasure of a deceased data subject's personal information, unless the deceased whilst he or she is alive provides otherwise.

RIGHT TO DATA PORTABILITY: The data subject has the right to request a handler to transfer his personal information to another handler provided that such transfer satisfies the requirements of the Cybersecurity Administration of China ("CAC"). It is worth noting that the PIPL has not prescribed what the CAC's requirements could be.

RIGHT TO REDRESSAL: The final version of the PIPL has included an additional right for the data subject, if a personal information handler refuses to comply with the request of a data subject, the data subject may seek redress in courts.

AUTOMATED DECISION MAKING: A data subject's right relating to automated decision making has been further expanded under the PIPL. The law expressly prohibits unreasonable different treatments on transaction terms, such as payments, by a handler if automated decision-making process is used.

RIGHT TO EXPLANATION AND REASON: The PIPL also sets out rights to individuals to request explanations from a handler on the data processing rules set by it. If a handler refuses any access request by an individual, the individual also has the right to request for an explanation.

RIGHT TO ACCESS AND RECTIFICATION: An individual has the right to access and request copies of his personal information from the personal information handler. This includes the right to rectify any inaccurate personal information and supplement incomplete personal information which the personal information handler holds.

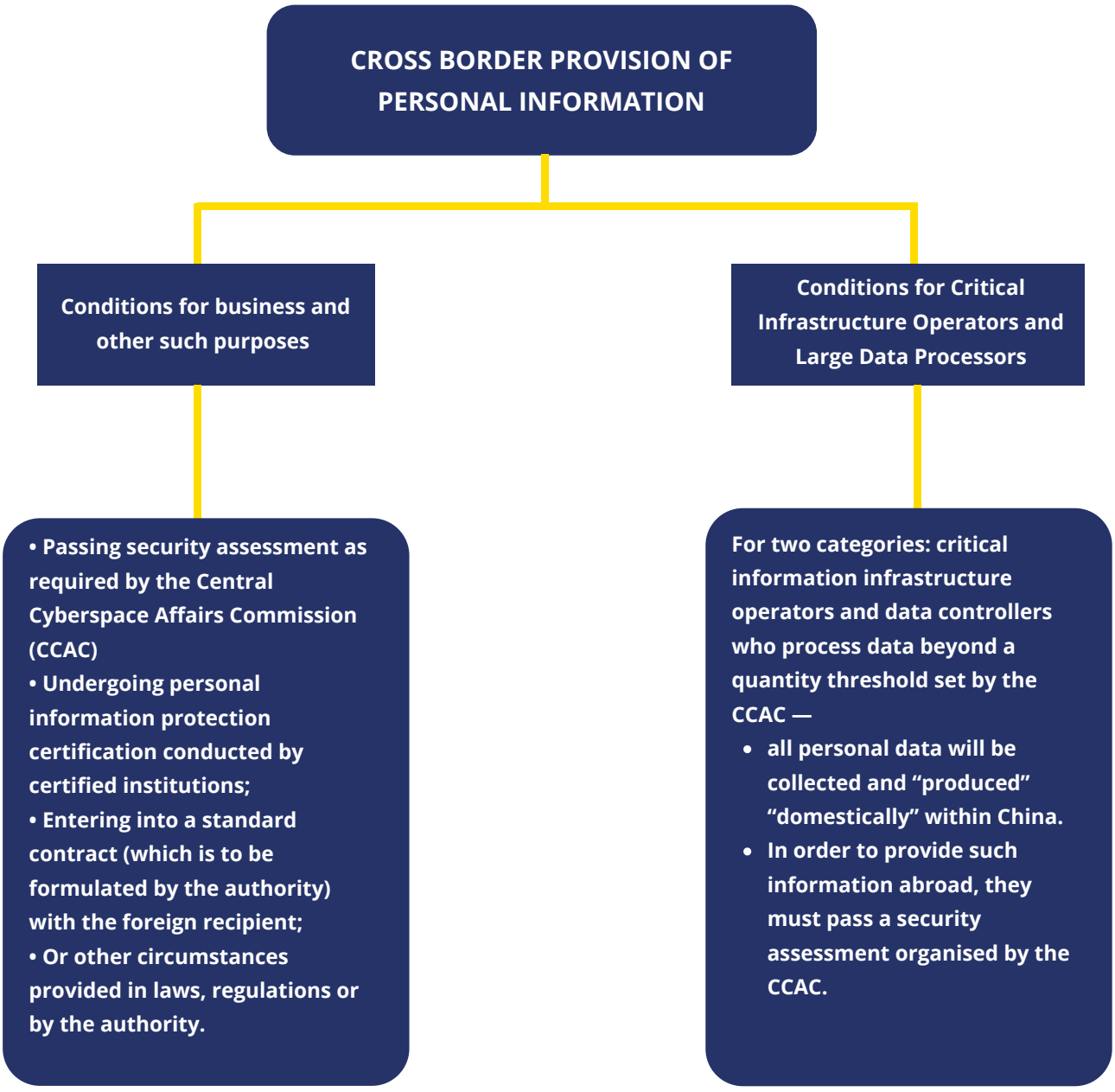
RIGHT TO ERASURE: An erasure request can be made to a handler when: the purposes for the personal information have been achieved or the agreed retention period has expired; handler ceases providing goods and services; consent has been revoked; and processing the data contrary to law or the agreed purposes.

DATA LOCALIZATION UNDER PIPL

Threshold for Storage of Personal Information:

The threshold required to store the personal information collected and generated within China by handlers, are as specified by the Cyberspace Administration of China (CAC). Unlike the requirements for Critical Information Infrastructure Operators (CIIO), there is no general data localization requirement on “important data” processed by non-CII operators in China.

CROSS-BORDER PROVISION OF PERSONAL INFORMATION



DIFFERENCES BETWEEN EU GDPR AND PIPL

CONSENT: Under EU GDPR, fresh consent for a new purpose may not always be required when there is another lawful basis for the new purpose. Under China PIPL, in case of change in the purpose and method of processing, fresh consent must be obtained.

CROSS-BORDER TRANSFER: Under GDPR, cross-border data transfers does not require further authorization, if the Commission has decided that such third country ensures an adequate level of data protection. Under PIPL, cross-border provision of personal information, some additional requirements, in particular the threshold that is to be reached, (security assessment) yet to be released by the CAC.

CRITERIA FOR PROCESSING PERSONAL INFORMATION: Under EU GDPR, Article 6 states the criteria for Lawful basis for processing activity under GDPR. China PIPL, does not provide "legitimate interests" as a lawful basis for processing as found in the GDPR. Instead, in addition to consent, Article 13 offers other requirements to be followed.

RIGHTS OF DATA SUBJECTS/INDIVIDUALS: The rights of the data subjects under the EU GDPR are quite similar to the rights of the individuals concerned under China PIPL. The right to data portability, has been provided under GDPR and PIPL, however, under the PIPL, this right is subject to the conditions formulated by CAC.

PENALTY: The penalty under GDPR is defined, and fines and penalties imposed under Article 83 are flexible and scale with the firm. Under China PIPL, the nature of remedies available are administrative, civil, and criminal. The PIPL does not specify whether the annual revenue refers to the worldwide turnover or the revenue generated in China.

CHALLENGES OF CHINA PIPL

Extra-Territorial Application

Extra-territorial organizations and business entities must ensure compliance with the establishment of a special agency or designate a representative within the territory of China, with certain responsibilities. This could adversely affect cross-border financial transactions or e-commerce transactions.

Mandatory Separate Consent

Given the limited time period till the enforcement of the PIPL, the fulfilment of “separate consent” from every individual whose personal information is being processed by the third-parties is tedious, also causing extensive delays.

Cross-Border Provision of Personal Information

The China PIPL strictly regulates the cross-border provision of personal information and, is permissible upon certain conditions having been met. This could be difficult to fulfil as certain processing activities occur during the course and cycle of the activities. It provides for reciprocating to any discriminatory, prohibitory or restrictive measures taken against the China pertaining to the protection of personal information.

Facial Recognition under PIPL

The PIPL provides for the image capturing and personal identification equipment to be permitted to be employed specifically for the purposes of maintaining public security. This restricts the scope of any such facial recognition measures or personal identification measures to the public space and does not mention private usage. This could obstruct the development of technological measures, with the evolution of facial recognition and other personal identification mechanisms.

Personal Information Handlers on a Large-Scale under PIPL

The personal information handlers providing important Internet Platform Services with a large number of users and complex business types are mandated to fulfill the enlisted obligations. Considering the large number of users and complexity of the business types, fulfilling these obligations would result in further complications due to constrained time period till the enforcement of the PIPL.

LEGAL LIABILITY

Consequences of illegal data processing: If the personal data processing is illegal or was done without adequate security measures in place, the relevant departments can order correction, confiscate illegal income, and issue a warning. If the personal information handler does not correct it, they may be fined an additional CN¥1 million (~₹1.1 crore) while the person directly in charge and other responsible personnel can be fined between CN¥10,000 (~₹1.1 lakh) to CN¥100,000 (~₹11 lakh).

Consequences of grave acts: If the illegal acts are "grave", the relevant departments can order correction, confiscate unlawful income, and impose a fine of up to CN¥50 million (~₹ 55 crores) or 5% of annual revenue. They may also suspend related business activities, report them to relevant authorities to get their business permits or professional licenses cancelled. The person directly in charge and other responsible personnel can be fined between CN¥100,000 (~₹ 11 lakh) to CN¥1 million (~₹1.1 crores).

Consequences to Government bodies: If government agencies do not fulfil their obligation, their superior organs or, departments will order correction, and people directly responsible will be disciplined as per law.

Consequences for illegally processing Chinese data abroad: If personal information handler illegally process personal data in China or of Chinese residents elsewhere in the world, they may be liable to pay CN¥50 million (~₹ 55 crores) or 5% of annual revenue in fines. In case any other countries take punitive actions against China in the field of personal data protection, China will retaliate in kind.

Compensation to users: If a personal information handler's processing activities violate a user's rights and interests, it is liable for compensating the loss that the individual suffer, due to such violation or the benefits received by the personal information handlers while processing the personal information.

CONCLUSION

The PIPL regime in China is the most awaited, as it introduces a legislation specifically pertaining to the subject-matter of personal data protection and privacy. It could not be disregarded that this law extensively aims at protecting the personal information of the individuals concerned, but poses challenges that could be potential hurdles while the law is being implemented from the perspective of organizations and business entities that process personal information. The PIPL allows exemptions favouring the government and, on the basis of laws and administrative regulations, that could also be viewed as a potential threat to personal data privacy.

BIBLIOGRAPHY

1. https://www.dataprotectionreport.com/2021/08/pipl-a-game-changer-for-companies-in-china/.

2. https://www.china-briefing.com/news/personal-information-protection-law-in-china-technical-considerations-for-companies/.

3. https://fpf.org/blog/chinas-new-comprehensive-data-protection-law-context-stated-objectives-key-provisions/.

4. https://www.lexology.com/library/detail.aspx?g=db4592e2-53c1-4cb6-91a9-94da1ee14b26.

5. https://www.medianama.com/2021/08/223-china-personal-information-protection-law/?utm_source=pocket_mylist.

6. https://iapp.org/news/a/analyzing-chinas-pipl-and-how-it-compares-to-the-eus-gdpr/

COMPANY PROFILE

Tsaaro provides privacy and cybersecurity services to help organizations meet regulatory requirements while maintaining a robust security infrastructure.

Our industry-standard privacy services include Privacy compliance, DPO-as-a-service, Vulnerability Assessment & Penetration Testing, Cyber Strategy, DPIA to name a few, delivered by our expert privacy professionals recognized by IAPP.

Secuvy is a global cloud based Data Privacy, Security and Governance company helping companies to automate Data Privacy workflows and building trust with their customers, which helps in avoiding millions in data privacy fines. Secuvy helps in finding, tracking and correlating Unstructured/Structured data for an individual in a single pane of glass with no rules and policies. Our Privacy Data Classification module helps in Data Minimization and Cross Border data transfer issues with respect to Global Privacy laws.

tsaaro

- **Akarsh Singh**

(CEO & Co-Founder Tsaaro)
Akarsh is a fellow in Information Privacy by IAPP, the highest certification in the field of privacy. His expertise lies in Data Privacy and Information Security Compliance.

- **Krishna Srivastava**

(Co-Founder & Head of Cyber Security Tsaaro)
Krishna is an ex-KPMG data security consultant. He has vast experience in Information Security and Data Privacy Compliance.

secuvy | ai

- **Vaibhav Mehrotra**

(CEO & Co-Founder Secuvy)
Vaibhav is an experienced Information Security Leader with a demonstrated history of building information security programs. He has experience in Data Privacy and Cyber Security.

CONTACT US

You can assess risk with respect to personal data and strengthen your data security by contacting Tsaaro.

Addresses:

Tsaaro India Office
Manyata Embassy Business Park,
Ground Floor, E1 Block,
Beech Building, Outer Ring Road,
Bangalore- 560045
India
P: +91-0522–3581306

Tsaaro Netherlands Office
Regus Schiphol Rijk
Beech Avenue 54-62,
Het Poortgebouw,
Amsterdam, 1119 PW,
Netherlands
P: +31-686053719

Email us:

info@tsaaro.com

secuvy | ai