TEKID
SECURING BUSINESS WITH INTELLIGENCE

China’s Personal Information Protection Law

Principles & impacts

February 23, 2022

Isabelle Hajjar
Head of Compliance - Cybersecurity & Privacy for TekID
Vice Chair - Cybersecurity Working Group - EUCC
CIPPE - CIPM

Data factors in China

Data is no longer a byproduct of technology but an economic resource

April 2020: "*Opinions on Improving the Mechanisms for Market-based Allocation of Production Factors*"

introduces the concept of "**Data factors**" - 数据要素

The term has been in every conversation around data in China for quite some time, and was even front and center in the 14th Five-Year Plan (2021-2025)

Beyond : Land, labor, capital, and technology, China has listed a 5th factor of production: "Data factors"

That means that, at the national policy level, China now has 5 official factors of production: land, labor, capital, technology, and **data**

By adding 'data' as a factor of production, Chinese policymakers are saying:

→ Data is as critical to our growth as the traditional four factors
→ We must create a well-ordered, well-regulated, standardized, stable market through which it can be bought, sold, shared, and used.

A four-pronged policy approach

Promote the open sharing of government data	**Enhance the value of data resources**	**Strengthen data resource integration and security protection**	Break (data) market monopolies

Source: Trivium China

China Cyber Regulations galore

TEKID
DIGITAL RISKS & SECURITY FIRM

- ✓ Guidelines for Personal Information Protection Within Information System For Public and Commercial Services (CSA)
- ✓ Amendment to the Law on the Protection of the Rights of Consumers (NPC)
- ✓ Provisions on Protecting the Personal Information of Telecommunications and Internet Users (MIIT)
- ✓ Regulation on Medical Records Management in Medical Institutions (NHFPC)

- ✓ Measures for Penalties for Infringing Upon the Rights and Interests of Consumers (SAIC)
- ✓ Amendment IX to the Criminal Law (NPC)
- ✓ Administrative Provisions on Short Message Services / SMS (MIIT)
- ✓ Administrative Measures for Online Payment Business of Non-Bank Payment Institutions (PBOC)
- ✓ National Security Law of the People's Republic of P.R.C. (NPC)

- ✓ Provisions on the Management of Mobile Internet Applications' Information Services (MIIT)
- ✓ Notice on Cleaning Up and Regulating the Internet Access Service Market (MIIT)
- ✓ Security Review Measures for Network Products and Services (CAC)
- ✓ Regulations on Internet Content Management Administration Law Enforcement Procedures (CAC)
- ✓ Administrative Measures on Internet News Information Services (CAC)
- ✓ Implementing Rules on the Licensing of Internet News Information Services (CAC)
- ✓ Catalogue on Critical Network Equipment and Specialised Network Security Products (First Batch) (CAC, MIIT, MPS, CNCA)
- ✓ Emergency Plan for National Cybersecurity Incidents (CAC)
- ✓ Administrative Measures for Evaluating Industrial Control System Information Security Protection Capability (MIIT)

- ✓ Decision on Strengthening Network Information Protection (NPC)
- ✓ GB/T 28448-2012 and GB/T 28449-2012 - Information Security Technology - Testing and Evaluation Requirement (TC260)

- ✓ Administrative Measures for Online Trading (SAIC)
- ✓ Administrative Measures for Population Health Information (NHFPC)
- ✓ Provisions on Application of Laws to Cases Involving Civil Disputes over Infringement upon Personal Rights by Using Information Networks (Supreme Court)

- ✓ Implementing Regulations of the Law on the Protection of Consumer Rights (SAIC) – Draft
- ✓ Interim Measures for the Administration of Internet Advertisements (SAIC)
- ✓ GB/T 20281-2015 and GB/T 20279-2015 Information security technology Security technical requirements (TC260)
- ✓ Administrative Provisions on Online Publication Services (MIIT)
- ✓ Notice on the Administration of Mobile Game Publishing (SAPPRFT)
- ✓ Telecommunications Regulations of PRC (2016 Revised) (SC)
- ✓ Administrative Rules for Internet Information Search Services (CAC)
- ✓ Mobile Internet Application Information Service Management Rules (CAC)
- ✓ Guidelines on the Information Security Protection of Industrial Control Systems (MIIT)
- ✓ Administrative Provisions on Internet Broadcasting Services (CAC)

- ✓ Administrative Provisions on Internet Forum Community Services (CAC)
- ✓ Administrative Provisions on Internet Post Comments Services (CAC)
- ✓ Administrative Measures for Internet Domain Name (MIIT)
- ✓ Administrative Provisions on Internet Group Information Services (CAC)
- ✓ Administrative Provisions on Internet User Public Account Information Services (CAC)
- ✓ Notice on Ensuring Policy Cohesion upon Removal of Four Administrative Approval Items, Including the Approval for Production of Commercial Encryption Products (SCA)
- ✓ Administrative Measures on Personnel Engaged in Content Management at Internet News Information Service Units (CAC)
- ✓ Administrative Provisions on Safety Assessment of New Technology and New Applications Relating to Internet News Information Services
- ✓ Emergency Plan for Emergent Cybersecurity Incident on the Public Internet (CAC)

And ….

✓ The Cybersecurity Law (CAC)

China Cyber Regulations galore

- ✓ Guiding Principles for Registration and Technical Evaluation of Medical Devices Cybersecurity (CFDA)
- ✓ Measures for the Monitoring, Delection and Handling of Public Network-related Network Security Threats (MIIT)
- ✓ Notice on Regulating Domain Name Usage by Internet Information Services (MIIT)
- ✓ GB/T 35273-2017 Personal Information Security Specification (TC260)
- ✓ Guidelines for Data Cross-border Transfer Security Assessment (TC260)
- ✓ GB/T 36630.1-2018 Controllability Evaluation Index for Security of IT products - Part 1 ： General Principles (TC260)
- ✓ GB/T 36630.2-2018 Controllability Evaluation Index for Security of IT Products - Part 2: Central Processing Unit (TC260)
- ✓ GB/T 36630.3-2018 Controllability Evaluation Index for Security of IT Products - Part 3: Operating System (TC260)
- ✓ GB/T 36630.4-2018 Controllability Evaluation Index for Security of IT Products - Part 4: Office Suite (TC260)
- ✓ GB/T 36630.5-2018 Controllability Evaluation Index for Security of IT products - Part 5: General Purpose Computer (TC260)
- ✓ Requirements for Implementation of Security Certification of Critical Network Equipment and Specialised Network Security Products (CNCA, CAC)
- ✓ Rules for the Implementation of Security Certification of Critical Network Equipment and Specialised Network Security Products (CNCA)

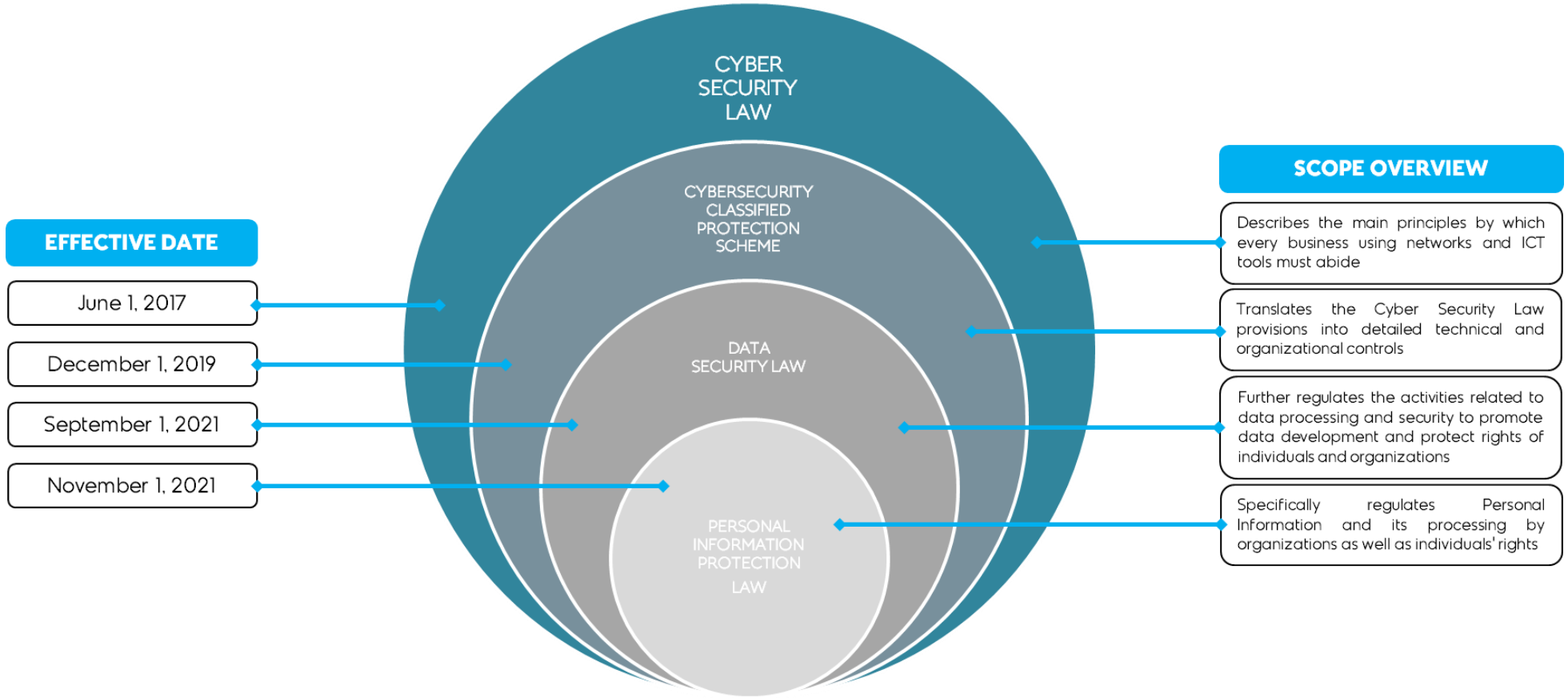
2018 | **2019**

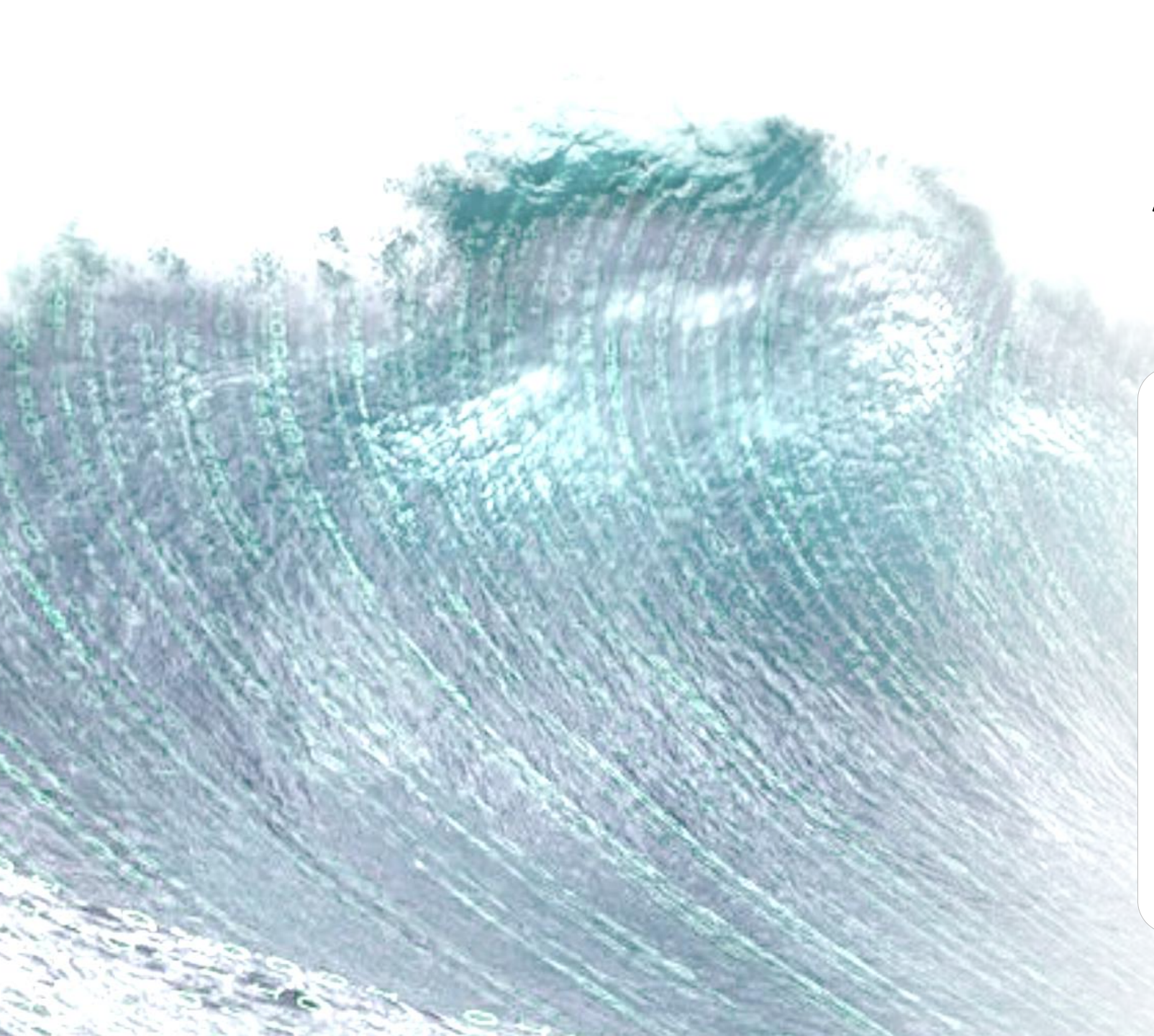
- ✓ *Supervision Rules for Insurance Institutions Adopting Digitalised Operations (SIRC)*
- ✓ *Minors Online Protection Regulations (CAC)*
- ✓ *Testing and Evaluation Process Guide for Cybersecurity Classified Protection (TC260)*
- ✓ *Testing and Evaluation Technology Guide for Cybersecurity Classified Protection (TC260)*
- ✓ *Requirements and Assessment Criteria Specification for Cybersecurity Classified Protection Testing and Evaluation Institutions*
- ✓ *Baseline for Cybersecurity Classified Protection (TC260)*
- ✓ *Evaluation Requirements for Cybersecurity Classified Protection(TC260)*
- ✓ *Notice on Regulating Market Behaviours of Cloud Service Providers (MIIT)*
- ✓ *Implementation Guide for Cybersecurity Classified Protection (TC260)*
- ✓ *Technical Requirements of Security Design for Cybersecurity Classified Protection (TC260)*
- ✓ *Interim Administrative Provisions on Internet and Information Security of Civil Aviation (CAAC)*
- ✓ *Cryptography Law of the People's Republic of China (SCA)*
- ✓ *Administrative Measures on Information Technology Used by Securities and Funds Operating Agencies (CSRC)*
- ✓ *Controllability evaluation index for security of information technology products - Part 1 ： General Principles (TC260)*
- ✓ *Controllability evaluation index for security of information technology products - Part 5: General Purpose Computer (TC260)*
- ✓ *Administrative Measures for Safety Assessment of New Internet-based Businesses (MIIT)*
- ✓ *Export Control Law of the People's Republic of China (MOFCOM)*
- ✓ *Regulations on Critical Information Infrastructure Protection (CAC)*
- ✓ *Guidelines for Personal Information De-identification (TC260)*
- ✓ *General Security Requirements for Network Products and Services (TC260)*
- ✓ *Indicator System of Critical Information Infrastructure Security Assurance (TC260)*
- ✓ *Guide to Security Inspection and Evaluation of Critical Information Infrastructure (TC260)*
- ✓ *E-Commerce Law (NPC)*

In a nutshell

China’s digital regulatory environment comprises laws, standards and guidelines which are imbricated within one another to provide additional specifications (being underlined that standards and guidelines are additional frameworks containing further requirements which are considered and enforced by authorities when evaluating the conformity of a company under certain regulations).

Assessing business operations in China against one of these regulations without consideration of the others would not provide you with a clear and understandable picture of the authorities’ expectations.





And now, the PIPL

- On the **1st of November 2021**, the Personal Information Protection Law (‘PIPL’) turned on. It sets a new bar in China for privacy rights, obligations, security, and compliance.
- The PIPL is China’s new data protection law. It is the **first China law focusing exclusively on personal data (omnibus law),** presenting many similarities with the European General Data Protection Regulation (‘GDPR’).
- At its core, the PIPL’s goals are to increase individuals’ rights and enhance privacy, transparency, and accountability. It does so by determining how personal data of China residents must be handled, what permissions are needed, and how such personal data can be lawfully collected, processed, and protected. It also gives individuals more rights and control over what can and cannot be done with their personal data.
- The PIPL also gives regulators new powers, including the possibility to impose significant fines on organizations that breach the law.

What is personal data?

Personal data is defined very broadly under the PIPL as ***any kind*** **of data that relates to an identified or identifiable natural person, whether in electronic form or recorded otherwise.**

Personal Data

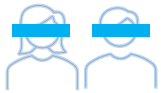
Classically understood personal data such as name, telephone number, address, ID number, etc.

Less obvious personal data, such as data related to a person's job, hair or eye color, style, opinions, comments, habits, likes and dislikes, activity logs, etc.

Sensitive Personal Data

Biometric characteristics, medical health, financial accounts, religious beliefs and individual location tracking

Specially designated status (Ex: -14 children data)

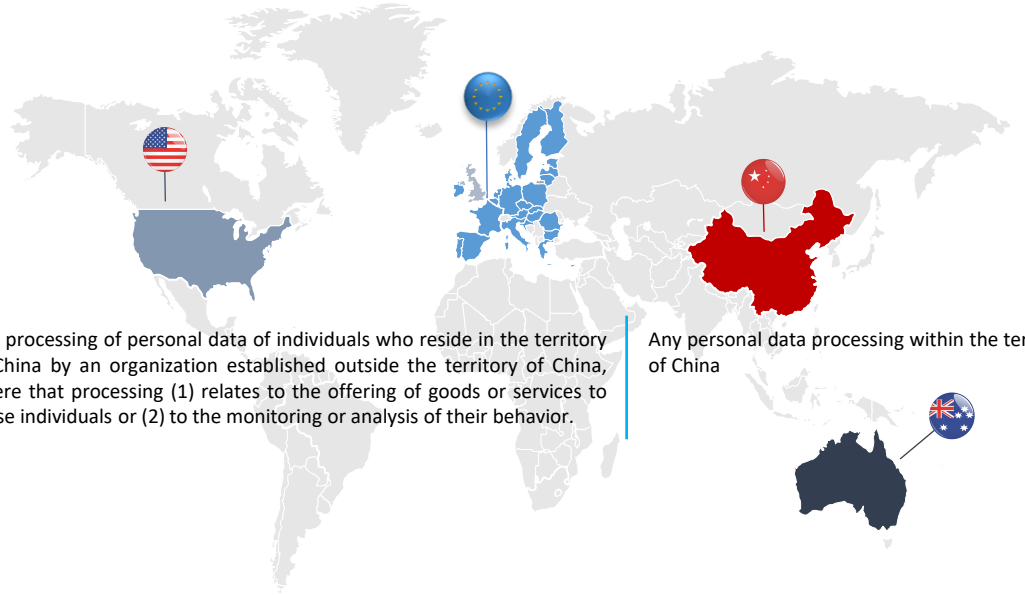


Anonymized Data ≠ Personal Data (Can be used freely)

Location tracking, being labelled '**sensitive personal data**' will present particular challenges for organizations and brands, as it will drastically reduce the extent to which they can, for example, track offline and online store visits for remarketing and retagging purposes.

Who and what does the PIPL apply to?

	Personal Data Handler	Personal Data Processor
WHO	If you are the one who **decides the purposes of personal data processing**	If you **process data on behalf of the Personal Data Handlers**
WHY	Because **<u>you are</u>** the one **deciding what can or cannot be done.**	Because you **<u>do not decide</u> the purposes of processing** and must **follow all instructions** given by the Personal Data Handlers.



Any processing of personal data of individuals who reside in the territory of China by an organization established outside the territory of China, where that processing (1) relates to the offering of goods or services to those individuals or (2) to the monitoring or analysis of their behavior.

Any personal data processing within the territory of China

PUT SIMPLY:
the PIPL applies to **any organization or business processing personal data of a China resident**. This **applies no matter where in the world your organization is based**, whatever its size or industry **(extra-territorial reach)**.

Your organization's core obligations?

You are a Personal Data Handler

In short, the PIPL shapes the responsibilities for the Personal Data Handlers and what they are accountable for. The Personal Data Handlers must **demonstrate that personal data is**:

Processed lawfully, legitimately, for necessity **(purpose limitation),** in good faith and in an open and transparent manner

Processed for specified (thorough information given to individuals), **reasonable, explicit and legitimate purposes**

Adequate, relevant, and limited to what is necessary: processing must not be excessive, and limited to the minimum scope necessary to achieve the explicit purpose **(data minimization and processing minimization)**

Of quality: i.e., accurate, complete and up to date;

Kept no longer than necessary (retention limitation)

Processed in a manner that ensures its **security**.

An internal management organization and rules

Personal data Classification	Training and awareness	Technical measures	Incident response plan
DPO or Privacy Rep	Audits	DPIAs	Breach notifications

You are a Personal Data Processor

The PIPL requires Personal Data Processors to **adopt necessary measures to ensure the security of personal data in accordance with relevant laws and regulations**, and to assist personal information handlers in fulfilling their obligations under this law.

Their personal data processing activities must be **supervised by the Personal Data Handlers** entrusting them with such processing.

Lawful processing - what does it mean?

						
Consent	**Contract**	**Legal Obligation**	**Health**	**News & Public Interest**	**Public Personal Data**	**Other Authorized circumstances**
Consent to the processing for specific purposes	For the conclusion or performance of a contract, or for **HR management**	For compliance with a legal or statutory obligation	For public health emergencies or for the protection of the life, health, and property of the individual	Within a reasonable scope, for news reporting, activity for public interest purposes	Within a reasonable scope, personal data that has been publicly disclosed by the individual or legally by a third party	...

What rights for individuals?

TEKLD
DIGITAL RISKS & SECURITY FIRM

Information

Truthful, accurate and full information on why, how and by whom personal data will be processed

Access & Copy

Right to receive a copy of the personal data processed by the Personal Data Handler

Correct & Complete

Inaccurate or incomplete personal data

Portability

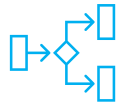
Right to request transmission to another Personal Data Handler, so long as the transfer meets conditions to be set by the CAC

Consent withdrawal

Right to withdraw consent at any Time

Deletion

Processing purpose achieved; personal data no longer necessary; provision of products / services has ceased; retention period expired; consent withdrawn;, violation of applicable laws and regulations



Not to be subject to automated decision-making

Right to request human intervention

Right to restrict or object

To processing of personal data

DSARs & Complaints

Submit requests *to Personal Data Handlers as to exercise their rights,*

File a lawsuit where such requests are rejected

What about cross-border data transfer?

The PIPL, and the recent issued measures on Security Assessment of the Cross-border Data Transfer (Draft) strictly regulate transfers of personal data of China residents outside of China

If I collect personal data in China and plan to transfer data to other countries :

China digital regulatory environment

In line with the Cyber Security Law, the Data Security Law and the PIPL require that Critical Infrastructure Information operators ('CIIOs'), as well as any other Personal Data Handler who processes personal data that reaches **a certain volume**, must:

- Store data (i.e., Including personal data) within the territory of China, and
- Where cross-border transfer of personal data is necessary, such transfer must pass a **security assessment** under the supervision of the CAC.

Complemented by

Measures on Security Assessment of the Cross-border Data Transfer of Personal and Important Data (Draft)

These measures further define circumstances where Personal Data Handlers transfering personal data overseas **must submit the security assessments for approval to authorities**.

Check by answering the following questions:

1. Am I a Critical Infrastructure Information Operator (CIIO)?

YES **NO** Check the next question

2. As far as personal data is concerned, do I either (or all):

- **Process more than 1,000,000 personal data in China and export personal data (whatever the exported volume)?**
- **Export over 100,000 personal data?**
- **Export over 10,000 sensitive personal data?**

YES **NO:**

If at least one "YES", you need to submit the security assessment for approval to authorities

If "NO" to both, you do <u>not</u> need to submit the security assessment for approval to authorities

In any case, any export of Personal Data must trigger an Impact Assessment.

As to 'important' data generally, it is defined as information that could pose a threat to national security, economic stability, and technological advancement, or significantly impact China's industrial and telecommunication sectors. However, China has yet to provide specific examples, leading to some uncertainty.

Your risks?

For the last few decades, Chinese laws have generally not included significant fines for breaches of privacy-related provisions. That changes dramatically under the PIPL.

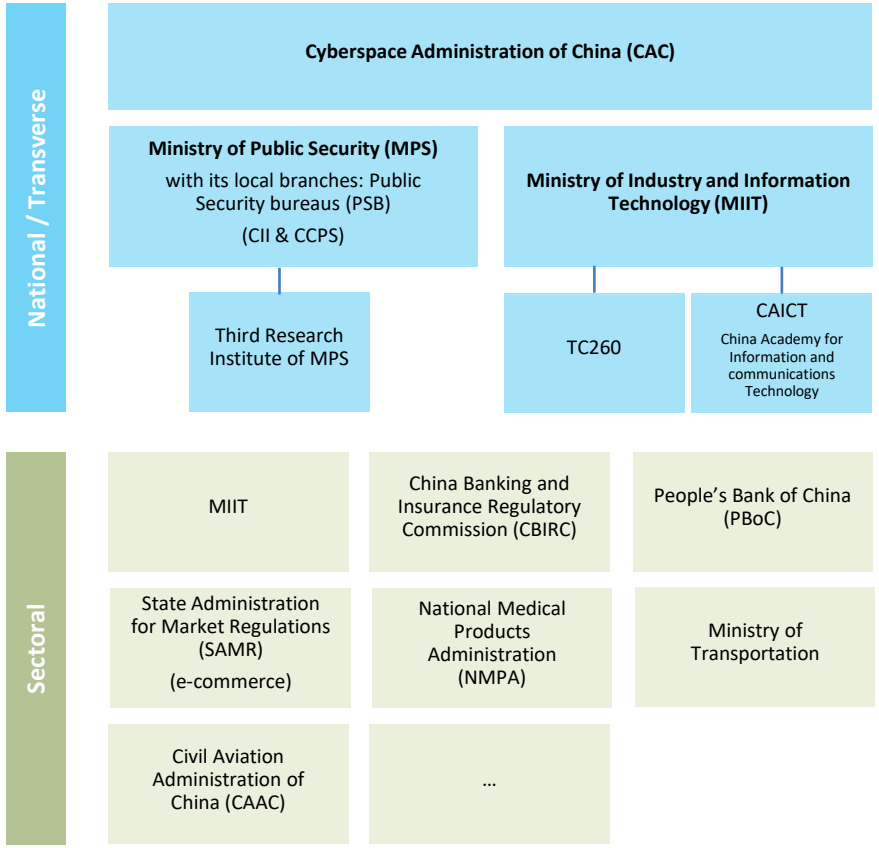
Fines for breaches of privacy-related provisions	Notable additional risks
The maximum fine for serious infringements will be the greater of **CNY 50 million (€ 6.9 Mil. / $7.9 Mil.) or 5% percent of an organization's annual revenue for the previous year**. In addition, an organization can face confiscation of illegal gains, suspension of related activities or even suspension of revocation of their business license and/or business permit.	**Any person in charge** or directly liable for the breach may also be fined up to **CNY 1 million** and may also be **barred from serving as director, supervisor, senior officer or data protection officer for a certain period**. Breaches which also constitute breaches of public security may be subject to sanctions under public security administration laws Breaches which constitute criminal acts may be subject to criminal prosecution (with imprisonment of up to **7 years**).

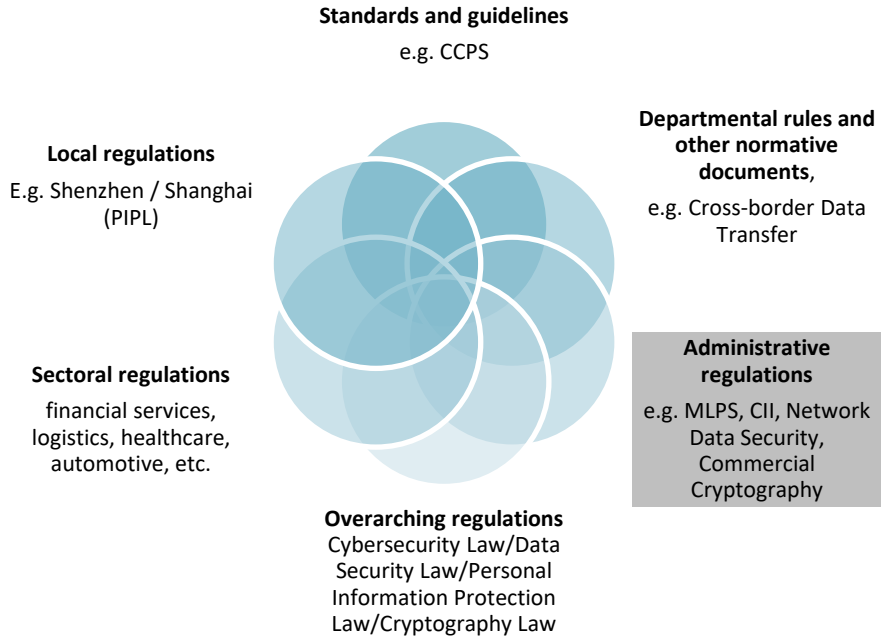
Challenges & Impacts

No one-stop shop

Multiple players: national & sectoral regulators - overarching and sectoral regulations

Multiple geographic regulatory layers: national, provincial regulations, district rules, etc.





Challenges & Impacts - Ignore the PIPL at your peril

TEKLD
DIGITAL RISKS & SECURITY FIRM

A 360° Regulatory Approach

The PIPL must not be approached in a vacuum.

The PIPL may be used as an entry point, but organizations take into account other laws, regulations and legal instruments which touch upon this area. Organizations must also be on the look out for additional texts that shed some light on certain concepts and notions.

E.g.:

- Already in 2021: China defined **'necessary' personal information that mobile apps can collect** for the basic functions and services of mobile apps.
- end August 2021: the '*Internet Information Service* ***Algorithm*** *Recommendation Management Regulations'*
- **Shanghai's & Shenzhen's recent local data regulations** (Jan. 2022), the first of their kind to be passed by a local government in China
- 13th of January 2022: the *'draft Guidelines for* ***Identification of Critical Data***', with shed light on the identification of critical data (i.e., 'important data') and core data.
- Etc.

Enforcement

Beijing just listed another 107 apps for data violations, incl, apps of Xiaomi, hotel booking apps of Shangri-La, IHG and Super 8, of online clinical service from Chinese insurer Taikang, and of Offcn Education.

Also listed: **13 software development kits** over the illegal collection of user data. (incl. those for Baidu's location service, ByteDance's ad platform Ocean Engine, and NetEase QiYu, a customer service and marketing solution under video gaming giant NetEase Inc.

The MIIT said they violated several laws, including the CSL and the PIPL and gave them until Feb 25 to correct the problems or face punishment.

There have been **21 such lists since 2019.** To date, the regulator has officially singled out and warned **over 1,862 mobile apps were warned and 643 of them (34.5%) were delisted**.

Since 2018: the Clean Internet crackdown on cybercrime, personal data infringements, etc. Just in In 2019: more than 45,000 cybercrime cases detected and over 65,000 suspects arrested.

⚠ Overseas companies that don't fall into line with the PIPL or harm the national security of China may be placed on a blacklist, which could effectively ban them from processing Chinese personal data.

A Growing Influence

China's influence is growing, and other countries are emulating its laws.

Such is the case, for example, of Vietnam (Cybersecurity Law).

The tit-for-tat retaliation provisions included in the PIPL are also eyed with interest by other countries (Vietnam, India).

So are the data localization obligations.

A global approach is necessary.

Leveraging

Organizations already **compliant with the GDPR** will have an advantage, as adaptation to the PIPL, as far as individuals' rights are concerned, will be made much easier. For the others, the gap may present difficult and important challenges (whether organizational, operational or technical).

Where compliant with the GDPR, organizations will need to address 'deviations' (location tracking is sensitive personal data, legitimate interests are not a legal basis, push marketing or sales are based on automated decision-making, cross-border transfer, etc.)

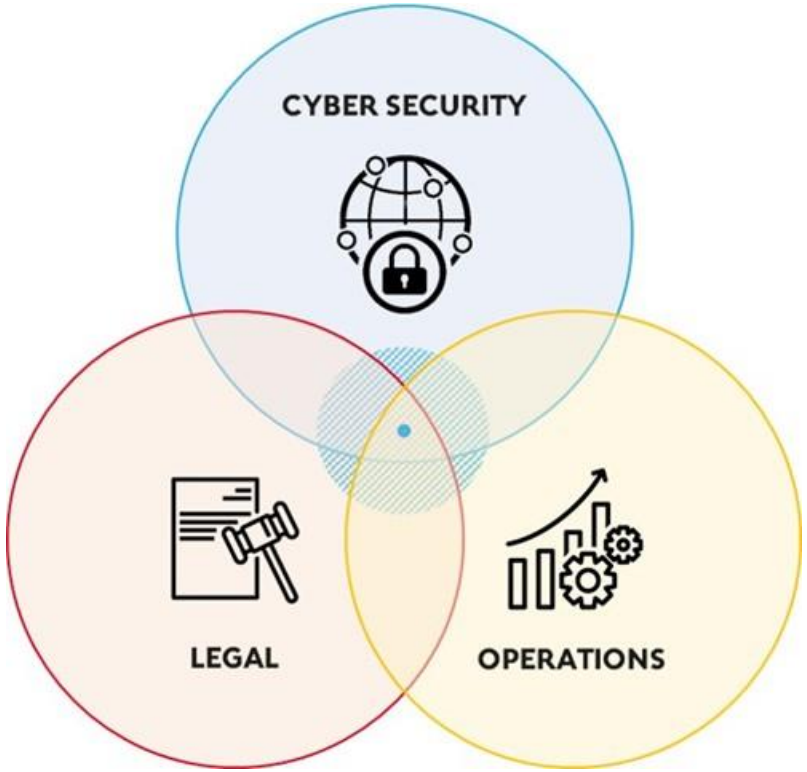
As to security: core security controls are the same wherever you are.

About us

DIGITAL RISKS & SECURITY FIRM
ADVISORY / CONSULTING / ENGINEERING

We are a **Digital Risks and Security firm** focusing on protecting the interests of our customers operating in the Cyberspace. We provide advisory, consulting and engineering services for multinational companies as well as medium-sized enterprises. Priding ourselves with a large spectrum of highly valued services, **our uniqueness resides in our tri-expertise** in legal, security and operations, that only a lean, cross-trained, imaginative and adaptable team can provide, together with the additional personal attention and hands-on executive involvement.
TEKID business core is rooted in the absolute willingness to best protect and advise our customers on the underlying risks of an exponential digital society.

We secure your business with intelligence.



VIGITRUST / TEKID