



Establishing comprehensive personal information protection management system

Personal Information Protection Law of the People's Republic of China (PIPL)
Challenges and Strategies

kpmg.com/cn



Recap of Personal Information Protection Law (PIPL)

Personal Information Protection Law of the People's Republic of China (hereinafter referred to as "PIPL") was approved at the 30th meeting of the Standing Committee of the 13th National People's Congress on August 20, 2021, and would come into effect on November 1, 2021, after nearly two years of preparation and three rounds of review. Compared with the 1st and the 2nd draft, key updates in the approved version are covering legal basis of personal information processing, protection obligations of personal information processors, personal information cross-border transfer, legal liability, etc..

Scope of application



- Personal information processing activities conducted within China
- Certain processing activities conducted outside of China, of domestic natural persons' personal information

Processor



- Organizations and individuals who independently decide the purpose and method of processing personal information.
- "Special" processors: joint processing, entrust and entrusted processing, third parties, etc.

Legal basis



- Obtain personal consent
- Signing or performing contracts, **or conducting human resources management based on legal documentation;**
- **Processing disclosed personal information within a reasonable scope within PIPL;** or
- Performing legal duties or obligations, responding to emergencies, implementing news reports and public opinion supervision for public interests, and other circumstances stipulated by laws and administrative regulations.

Protection obligations



- Protection from organization & people, policy & procedure, and technology enabled etc.
- Additional requirements in processing sensitive personal information, **establishment of specific personal information processing rules when processing personal information of children under 14**
- Responding and addressing individual's applications for the exercise of rights, **and the right of personal information portability, the exercise of rights when a natural person is deceased, etc.**
- Pre-event **personal information protection impact assessment** and **regular compliance audit**

Cross-border transfer



- Critical Infrastructure Information Operator (CIIO) and personal information processors who reach the number prescribed by the State Cyberspace Administration shall store the personal information collected and generated within China
- Pre-conditions: Passed the security assessment organized by the authority, achieved personal information protection certification by authorized agencies, **signed a standard contract formulated by the authority with the overseas receiver(s)** to agree upon the rights and obligations, etc.
- Pre-event **personal information protection impact assessment** and separate consent, and **the personal information protection capabilities of the overseas receiver(s) up to the standards in PIPL**

Legal liability



- Ordering rectification, confiscating illegal gains, fines for organizations and people, recording in the credit profiles, compensating for losses, etc.
- **Ordering to suspend or terminate the services provided by the applications illegally processing personal information**
- The maximum fine is not more than 50 million yuan or not more than 5% of its turnover of the previous year
- The fine to the directly responsible person is 100,000 to 1 million, **and the person could be prohibited to be a director, supervisor, senior manager, or personal information protection officer of relevant enterprises within a certain period**

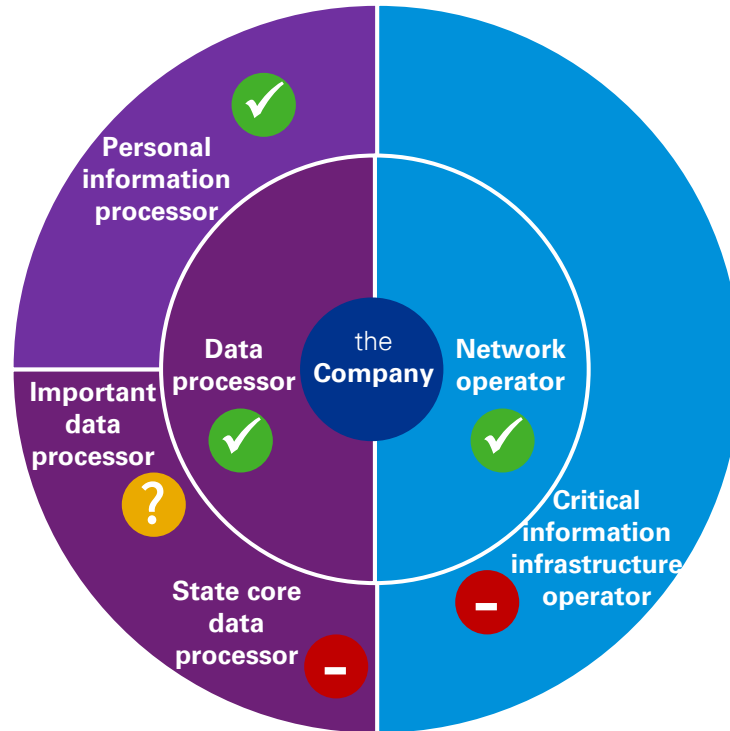
中华人民共和国 网络安全法 (网安法) Cybersecurity Law of the People's Republic of China (CSL) 2017年6月1日生效 Enacted June 1st, 2017	中华人民共和国 数据安全法 (数安法) Data Security Law of the People's Republic of China (DSL) 2021年9月1日生效 Enact from September 1st, 2021	中华人民共和国 个人信息保护法 (个保法) Personal Information Protection Law of the People's Republic of China (PIPL) 2021年11月1日生效 Enact from November 1st, 2021
---	--	--

When it comes to topic of "personal information protection", China Personal Information Protection Law shall be followed, which shall be more "comparable" with other data protection laws and regulations across the world like EU GDPR, US CCPA, etc.

Source: KPMG analysis

Notes: The bold part is summarized from key updates in the approved version of PIPL.

Understanding different roles of a Company in cybersecurity and data protection



Companies basically would be considered as **network operators** (CSL), **data processors** (DSL) and **personal information processors** (PIPL)



Some companies may be involved in the processing of important data

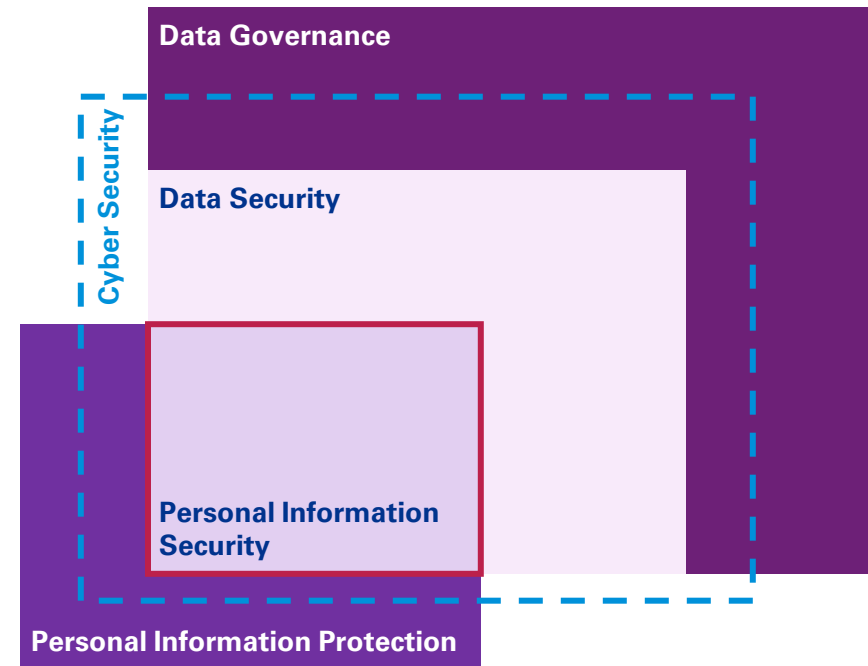


Limited companies may be involved in the processing of state core data and/or operate critical information infrastructure



To address basic compliance requirements, Companies shall establish and improve the following:

1. Information Security Management System
2. Data Security Management System; and
3. Personal Information Management System



Source: KPMG analysis

Quick summary – PIPL vs EU GDPR



Scope of application	PIPL focuses on the territory of personal information processing activities, while EU GDPR focuses on data controller / processor setup location
Personal information processor	“Processor” and special type of “Processor” in PIPL; “Controller” & “Processor” in EU GDPR - Minor differences for the definition of sensitive personal information between PIPL and EU GDPR
Legal basis	- PIPL includes the processing of disclosed personal Information within a reasonable scope - PIPL specifies the processing that necessary to conduct human resources management based on legally formulated labour documentation - PIPL requires to obtain separate consent in certain personal information processing scenarios
Protection obligations	- Minor differences in privacy notice content between PIPL and EU GDPR - PIPL requires to establish specific personal information processing rules when processing personal information of children under 14 - Minor differences for data subject rights between PIPL and EU GDPR, especially for the request for the explanation of PI processing rules and the exercise of rights when a natural person is deceased in PIPL - PIPL requires personal information classified protection - Minor differences for the trigger conditions on personal information protection impact assessment and the record retention period between PIPL and EU GDPR - PIPL specifies personal information processing requirements regarding APP, “Big data price discrimination”, image capturing in public places, etc. - PIPL requires to establish a dedicated organization or assign a representative within China if domestic personal information is processed

Personal information cross-border transfer	- Pre-conditions of cross-border transfer in PIPL, including: 1) passed the security assessment organized by the authority, 2) achieved personal information protection certification by authorized agencies, 3) signed a standard contract formulated by the authority with the overseas receiver(s) or 4) other conditions stipulated by laws, regulations or the authority - PIPL requires the personal information protection capabilities of the overseas receiver(s) up to the standards in PIPL - PIPL specifies that CIO and personal information processors who reach the number prescribed by the State Cyberspace Administration shall store the personal information collected and generated within China - PIPL requires to perform pre-event personal information protection impact assessment and obtain separate consent
Legal liability	More severe legal liability in PIPL, including ordering rectification (ordering to suspend or terminate the services provided by the applications), confiscating illegal gains, fines for organizations and people, business banning for the senior management, recording in the credit profiles, compensating for losses, etc.

Notes: EU GDPR refers to *General Data Protection Regulation* in EU.

Quick summary – PIPL vs GB/T 35273-2020 (“PISS”)

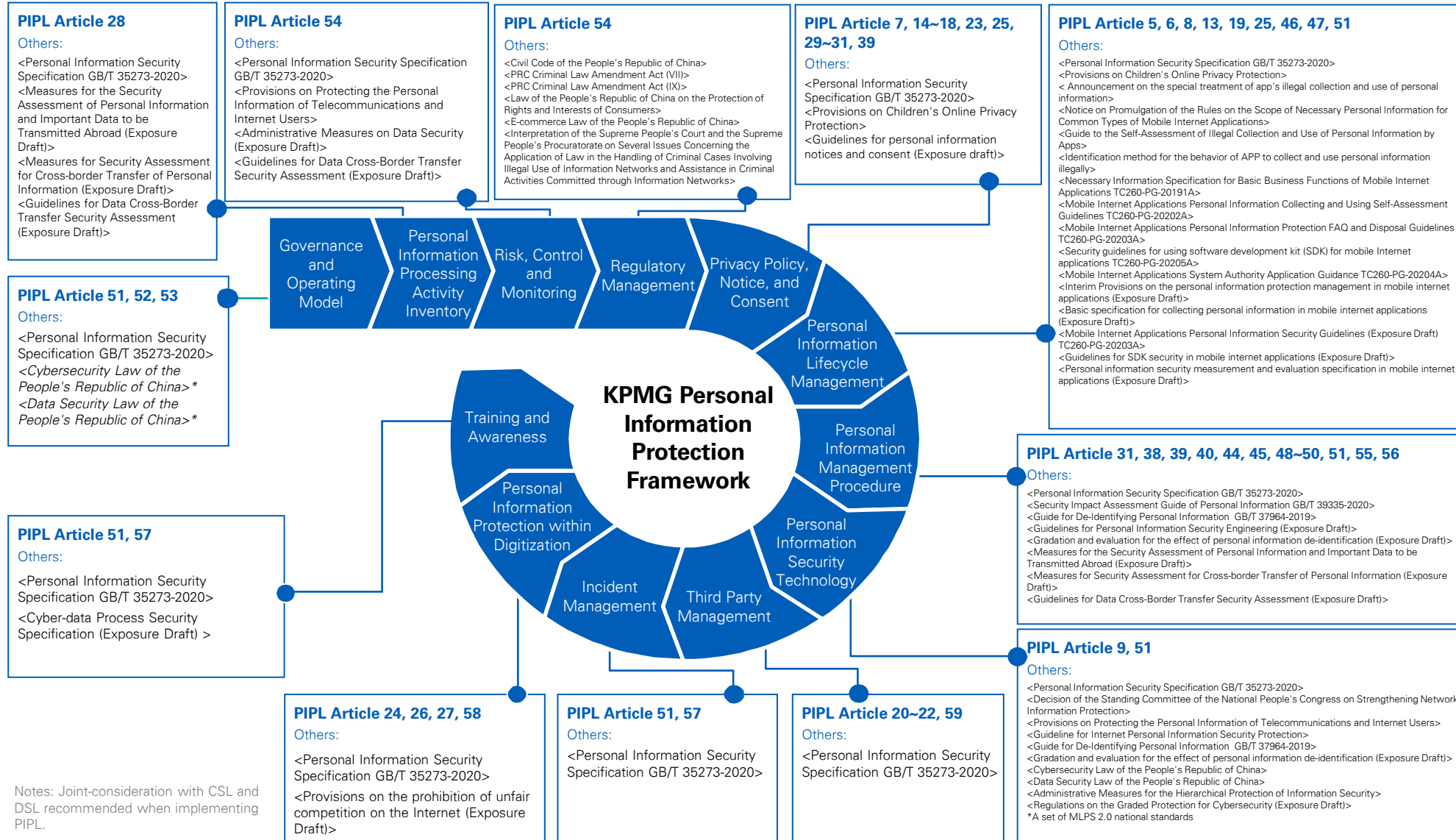
Scope of application	• -
Personal information processor	• “Processor” and special type of “Processor” in PIPL; “Controller” in PISS
Legal basis	• Minor differences in exceptions to obtaining consent between PIPL and PISS PIPL includes the processing of disclosed personal Information within a reasonable scope; or necessary to conduct human resources management based on legally formulated labour documentation
Protection obligations	• PIPL requires to establish specific personal information processing rules when processing personal information of children under 14 • Minor differences for data subject rights between PIPL and PISS, especially for the right to know, right to request for the explanation of PI processing rules and the exercise of rights when a natural person is deceased in PIPL • PIPL requires personal information classified protection • Minor differences for the trigger conditions on personal information protection impact assessment and the record retention period between PIPL and PISS • PIPL specifies personal information processing requirements regarding APP, “Big data price discrimination”, image capturing in public places, etc. • PIPL requires to establish a dedicated organization or assign a representative within China if domestic personal information is processed

Personal information cross-border transfer	• Pre-conditions of cross-border transfer in PIPL, including: 1) passed the security assessment organized by the authority, 2) achieved personal information protection certification by authorized agencies, 3) signed a standard contract formulated by the authority with the overseas receiver(s) or 4) other conditions stipulated by laws, regulations or the authority • PIPL requires the personal information protection capabilities of the overseas receiver(s) up to the standards in PIPL • PIPL specifies that CIIO and personal information processors who reach the number prescribed by the State Cyberspace Administration shall store the personal information collected and generated within China • PIPL requires to perform pre-event personal information protection impact assessment
Legal liability	• -

Notes: GB/T 35273-2020 refers to *Information security technology - Personal information security specification*



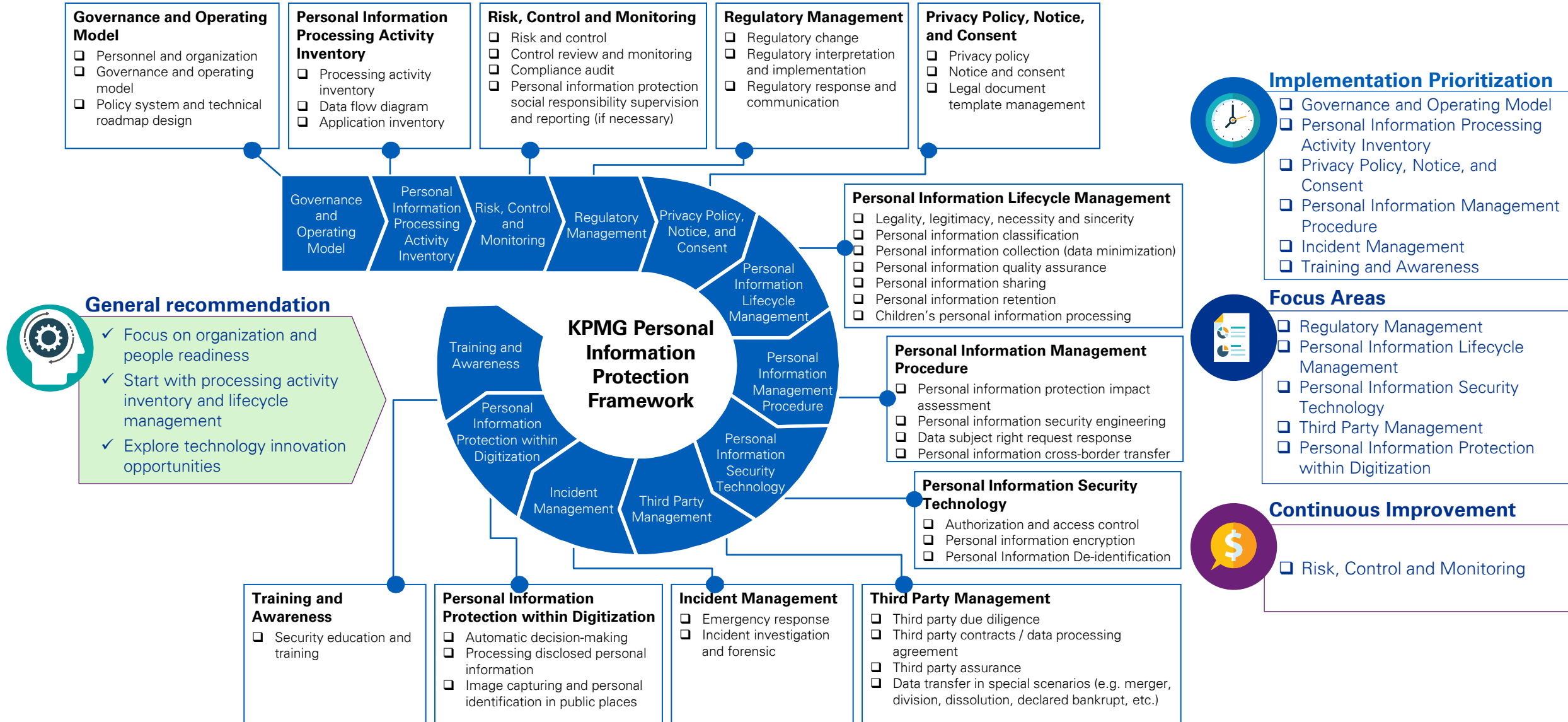
Understand personal information protection requirements



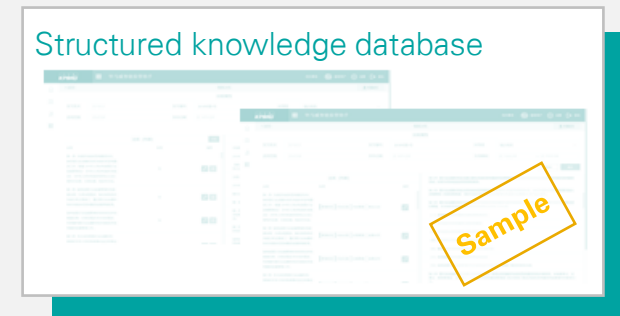
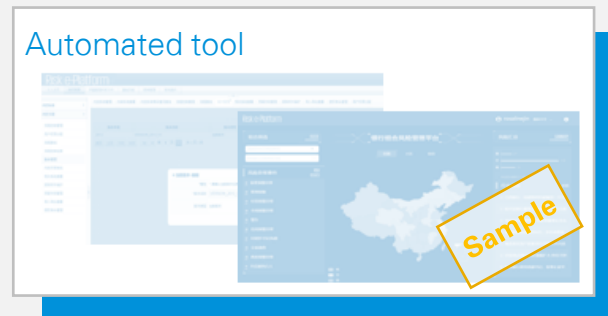
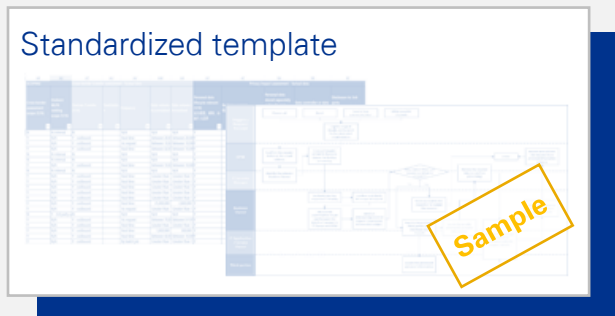
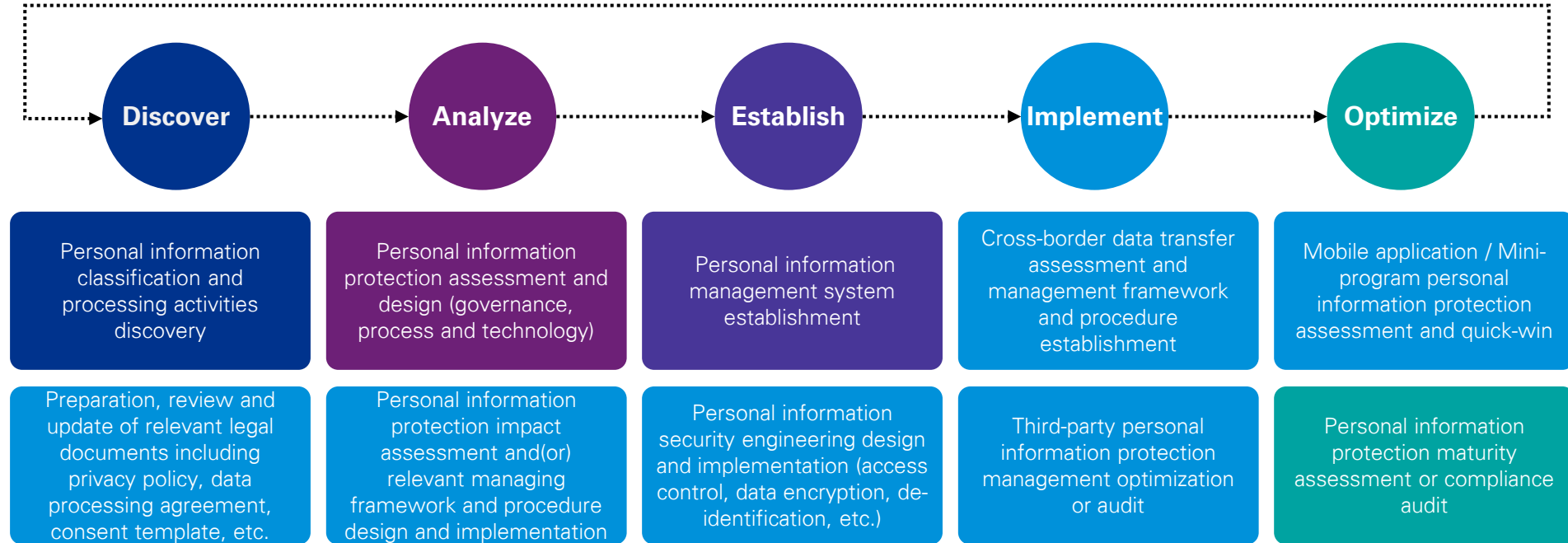
Departments Fulfilling Personal Information Protection Duties and Responsibilities

- ❖ **National cyberspace authority**
Responsible for comprehensive planning and coordination of personal information protection work and related supervision and management work
- ❖ **State Council relevant departments**
Responsible for Personal Information protection, supervision, and management work within their respective scope of duties and responsibilities, according to the provisions of this Law and relevant laws and administrative regulations
- ❖ **County-level and higher People's Governments relevant departments**
The personal Information Protection, supervision, and management duties and responsibilities are determined according to relevant State regulations

Establish personal information protection management system



Our services along the journey



Henry Shek

KPMG China
Cybersecurity Advisory
Partner
Tel: +852 2143 8799
henry.shek@kpmg.com

Richard Zhang

KPMG China
Cybersecurity Advisory
Partner
Tel: +86 (21) 2212 3637
richard.zhang@kpmg.com

Brian Cheung

KPMG China
Cybersecurity Advisory
Director
Tel: +852 2847 5062
brian.cheung@kpmg.com

Quin Huang

KPMG China
Cybersecurity Advisory
Director
Tel: +86 (21) 2212 2355
quin.huang@kpmg.com

Danny Hao

KPMG China
Cybersecurity Advisory
Director
Tel: +86 (10) 8508 5498
danny.hao@kpmg.com





The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2021 KPMG Advisory (China) Limited, a limited liability company in China and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.