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**

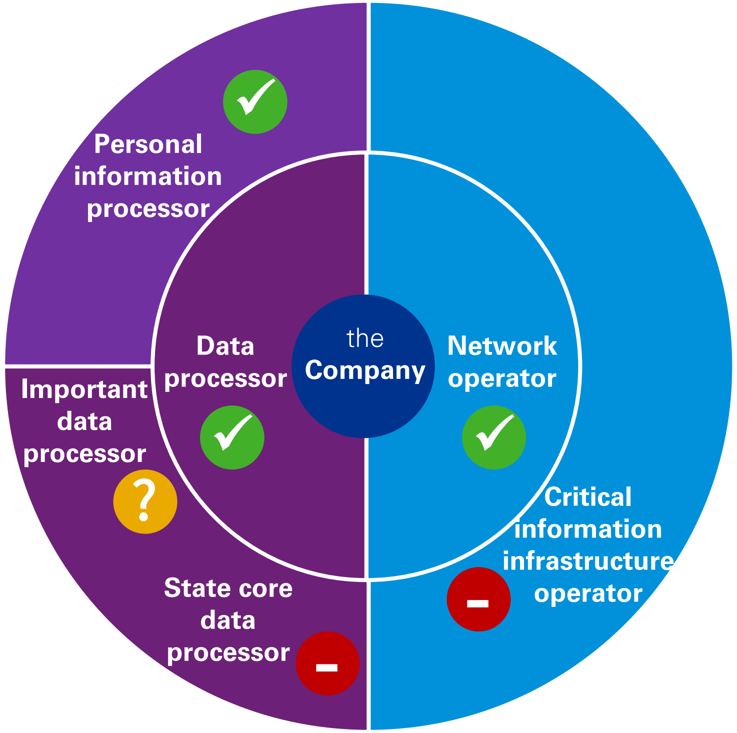
中华人民共和国 网络安全法 （网安法） Cybersecurity Law of the People's Republic of China (CSL) 2017年6月1日生效 Enacted June 1st, 2017	**中华人民共和国 数据安全法 （数安法） Data Security Law of the People's Republic of China (DSL)** 2021年9月1日生效 Enact from September 1st, 2021	**中华人民共和国 个人信息保护法 （个保法） Personal Information Protection Law of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



✓ Personal information processor
Important data processor ?
State core data processor –
Data processor ✓
the Company
Network operator ✓
Critical information infrastructure operator –

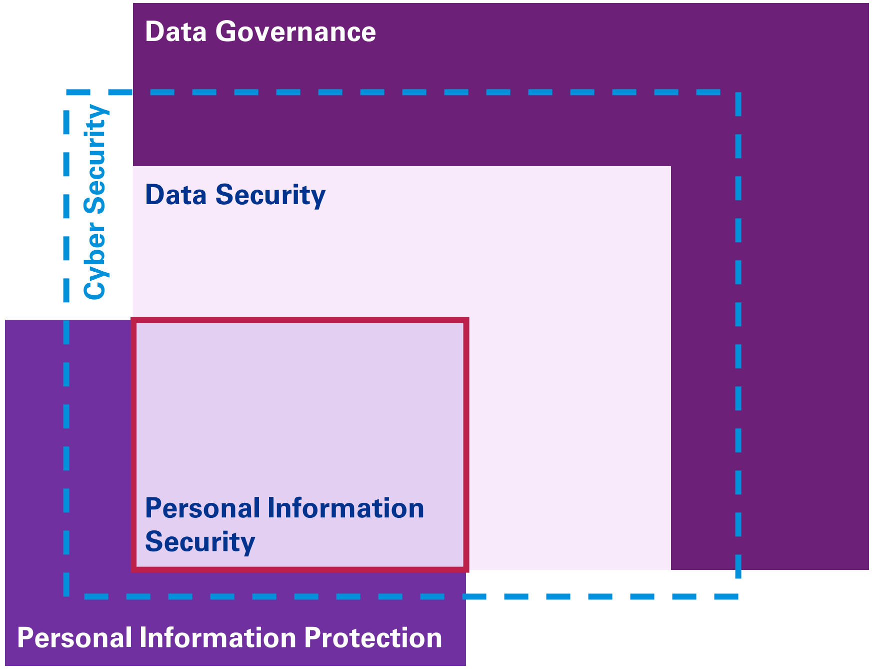
✓ Companies basically would be considered as **network operators** (CSL), **data processors** (DSL) **and personal information processors** (PIPL)

? 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



Data Governance
Cyber Security
Data Security
Personal Information Security
Personal Information Protection

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 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 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

PIPL Article 28

Others:

<Personal Information Security Specification GB/T 35273-2020>
<Measures for the Security Assessment of Personal Information and Important Data to be Transmitted Abroad (Exposure Draft)>
<Measures for Security Assessment for Cross-border Transfer of Personal Information (Exposure Draft)>
<Guidelines for Data Cross-Border Transfer Security Assessment (Exposure Draft)>

PIPL Article 54

Others:

<Personal Information Security Specification GB/T 35273-2020>
<Provisions on Protecting the Personal Information of Telecommunications and Internet Users>
<Administrative Measures on Data Security (Exposure Draft)>
<Guidelines for Data Cross-Border Transfer Security Assessment (Exposure Draft)>

PIPL Article 54

Others:

<Civil Code of the People’s Republic of China>
<PRC Criminal Law Amendment Act (VII)>
<PRC Criminal Law Amendment Act (IX)>
<Law of the People's Republic of China on the Protection of Rights and Interests of Consumers>
<E-commerce Law of the People’s Republic of China>
<Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in the Handling of Criminal Cases Involving Illegal Use of Information Networks and Assistance in Criminal Activities Committed through Information Networks>

PIPL Article 7, 14~18, 23, 25, 29~31, 39

Others:

<Personal Information Security Specification GB/T 35273-2020>
<Provisions on Children's Online Privacy Protection>
<Guidelines for personal information notices and consent (Exposure draft)>

PIPL Article 5, 6, 8, 13, 19, 25, 46, 47, 51

Others:

<Personal Information Security Specification GB/T 35273-2020>
<Provisions on Children's Online Privacy Protection>
< Announcement on the special treatment of app's illegal collection and use of personal information>
<Notice on Promulgation of the Rules on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications>
<Guide to the Self-Assessment of Illegal Collection and Use of Personal Information by Apps>
<Identification method for the behavior of APP to collect and use personal information illegally>
<Necessary Information Specification for Basic Business Functions of Mobile Internet Applications TC260-PG-20191A>
<Mobile Internet Applications Personal Information Collecting and Using Self-Assessment Guidelines TC260-PG-20202A>
<Mobile Internet Applications Personal Information Protection FAQ and Disposal Guidelines TC260-PG-20203A>
<Security guidelines for using software development kit (SDK) for mobile Internet applications TC260-PG-20205A>
<Mobile Internet Applications System Authority Application Guidance TC260-PG-20204A>
<Interim Provisions on the personal information protection management in mobile internet applications (Exposure Draft)>
<Basic specification for collecting personal information in mobile internet applications (Exposure Draft)>
<Mobile Internet Applications Personal Information Security Guidelines (Exposure Draft) TC260-PG-20203A>
<Guidelines for SDK security in mobile internet applications (Exposure Draft)>
<Personal information security measurement and evaluation specification in mobile internet applications (Exposure Draft)>

PIPL Article 51, 52, 53

Others:

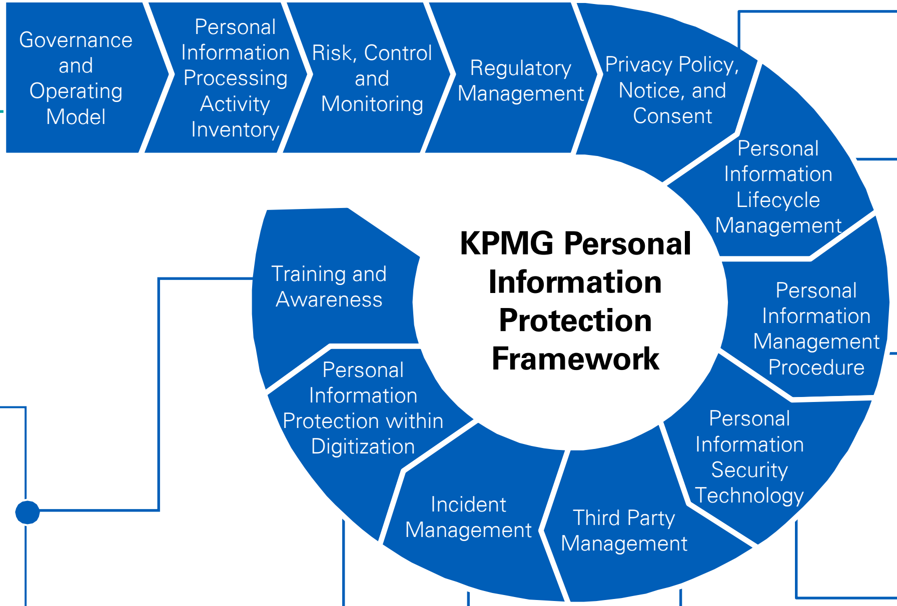
<Personal Information Security Specification GB/T 35273-2020>
*<Cybersecurity Law of the People's Republic of China>**
*<Data Security Law of the People's Republic of China>**

PIPL Article 51, 57

Others:

<Personal Information Security Specification GB/T 35273-2020>

<Cyber-data Process Security Specification (Exposure Draft) >



KPMG Personal Information Protection Framework

Governance and Operating Model

Personal Information Processing Activity Inventory

Risk, Control and Monitoring

Regulatory Management

Privacy Policy, Notice, and Consent

Personal Information Lifecycle Management

Personal Information Management Procedure

Personal Information Security Technology

Third Party Management

Incident Management

Personal Information Protection within Digitization

Training and Awareness

PIPL Article 31, 38, 39, 40, 44, 45, 48~50, 51, 55, 56

Others:

<Personal Information Security Specification GB/T 35273-2020>
<Security Impact Assessment Guide of Personal Information GB/T 39335-2020>
<Guide for De-Identifying Personal Information GB/T 37964-2019>
<Guidelines for Personal Information Security Engineering (Exposure Draft)>
<Gradation and evaluation for the effect of personal information de-identification (Exposure Draft)>
<Measures for the Security Assessment of Personal Information and Important Data to be Transmitted Abroad (Exposure Draft)>
<Measures for Security Assessment for Cross-border Transfer of Personal Information (Exposure Draft)>
<Guidelines for Data Cross-Border Transfer Security Assessment (Exposure Draft)>

PIPL Article 24, 26, 27, 58

Others:

<Personal Information Security Specification GB/T 35273-2020>

<Provisions on the prohibition of unfair competition on the Internet (Exposure Draft)>

PIPL Article 51, 57

Others:

<Personal Information Security Specification GB/T 35273-2020>

PIPL Article 20~22, 59

Others:

<Personal Information Security Specification GB/T 35273-2020>

PIPL Article 9, 51

Others:

<Personal Information Security Specification GB/T 35273-2020>
<Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection>
<Provisions on Protecting the Personal Information of Telecommunications and Internet Users>
<Guideline for Internet Personal Information Security Protection>
<Guide for De-Identifying Personal Information GB/T 37964-2019>
<Gradation and evaluation for the effect of personal information de-identification (Exposure Draft)>
<Cybersecurity Law of the People's Republic of China>
<Data Security Law of the People's Republic of China>
<Administrative Measures for the Hierarchical Protection of Information Security>
<Regulations on the Graded Protection for Cybersecurity (Exposure Draft)>
*A set of MLPS 2.0 national standards

Notes: Joint-consideration with CSL and DSL recommended when implementing PIPL.

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

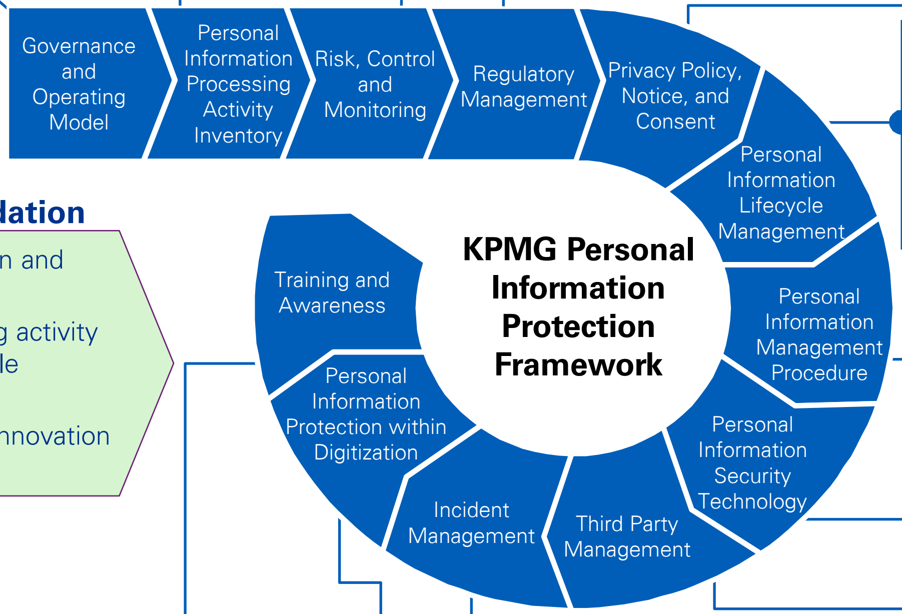
Governance and Operating Model
- ❑ Personnel and organization
- ❑ Governance and operating model
- ❑ Policy system and technical roadmap design

Personal Information Processing Activity Inventory
- ❑ Processing activity inventory
- ❑ Data flow diagram
- ❑ Application inventory

Risk, Control and Monitoring
- ❑ Risk and control
- ❑ Control review and monitoring
- ❑ Compliance audit
- ❑ Personal information protection social responsibility supervision and reporting (if necessary)

Regulatory Management
- ❑ Regulatory change
- ❑ Regulatory interpretation and implementation
- ❑ Regulatory response and communication

Privacy Policy, Notice, and Consent
- ❑ Privacy policy
- ❑ Notice and consent
- ❑ Legal document template management


Governance and Operating Model
Personal Information Processing Activity Inventory
Risk, Control and Monitoring
Regulatory Management
Privacy Policy, Notice, and Consent
Personal Information Lifecycle Management
Personal Information Management Procedure
Personal Information Security Technology
Third Party Management
Incident Management
Personal Information Protection within Digitization
Training and Awareness
KPMG Personal Information Protection Framework

Personal Information Lifecycle Management
- ❑ Legality, legitimacy, necessity and sincerity
- ❑ Personal information classification
- ❑ Personal information collection (data minimization)
- ❑ Personal information quality assurance
- ❑ Personal information sharing
- ❑ Personal information retention
- ❑ Children's personal information processing

Personal Information Management Procedure
- ❑ Personal information protection impact assessment
- ❑ Personal information security engineering
- ❑ Data subject right request response
- ❑ Personal information cross-border transfer

Personal Information Security Technology
- ❑ Authorization and access control
- ❑ Personal information encryption
- ❑ Personal Information De-identification

Training and Awareness
- ❑ Security education and training

Personal Information Protection within Digitization
- ❑ Automatic decision-making
- ❑ Processing disclosed personal information
- ❑ Image capturing and personal identification in public places

Incident Management
- ❑ Emergency response
- ❑ Incident investigation and forensic

Third Party Management
- ❑ Third party due diligence
- ❑ Third party contracts / data processing agreement
- ❑ Third party assurance
- ❑ Data transfer in special scenarios (e.g. merger, division, dissolution, declared bankrupt, etc.)

General recommendation

- ✓ Focus on organization and people readiness
- ✓ Start with processing activity inventory and lifecycle management
- ✓ Explore technology innovation opportunities

Implementation Prioritization

- ❑ Governance and Operating Model
- ❑ Personal Information Processing Activity Inventory
- ❑ Privacy Policy, Notice, and Consent
- ❑ Personal Information Management Procedure
- ❑ Incident Management
- ❑ Training and Awareness

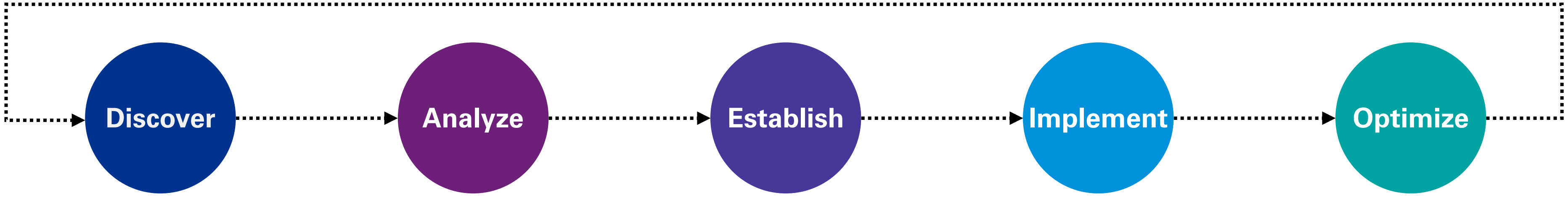
Focus Areas

- ❑ Regulatory Management
- ❑ Personal Information Lifecycle Management
- ❑ Personal Information Security Technology
- ❑ Third Party Management
- ❑ Personal Information Protection within Digitization

Continuous Improvement

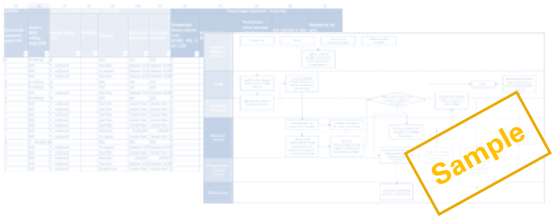
- ❑ Risk, Control and Monitoring

Our services along the journey



Discover	Analyze	Establish	Implement	Optimize
Personal information classification and processing activities discovery	Personal information protection assessment and design (governance, process and technology)	Personal information management system establishment	Cross-border data transfer assessment and management framework and procedure establishment	Mobile application / Mini-program personal information protection assessment and quick-win
Preparation, review and update of relevant legal documents including privacy policy, data processing agreement, consent template, etc.	Personal information protection impact assessment and(or) relevant managing framework and procedure design and implementation	Personal information security engineering design and implementation (access control, data encryption, de-identification, etc.)	Third-party personal information protection management optimization or audit	Personal information protection maturity assessment or compliance audit

Standardized template



Automated tool

Structured knowledge database

Contact us

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.