

ANJIE

安杰律师事务所

杰出 所以安心
DEDICATED
TO EXCELLENCE

BEIJING SHANGHAI HONGKONG SHENZHEN HAIKOU

ANJIELAW.COM

Introduction



Samuel Yang, Partner
AnJie Law Firm, China

Email: yanghongquan@anjielaw.com

Phone: +86 10 8567 2968

Mobile: +86 1391 0677 369

Wechat:



*Samuel leads the **Technology, Data Protection & Cyber Security** practice in AnJie Law Firm. He has nearly 20 years experience in these areas and is recognized as a leading lawyer by international legal directories including Chambers and Partners, Legal 500, Who's Who Legal and LEGALBAND.*

Before he joined AnJie, he worked for DLA Piper, CMS and British Telecom

Sun Li, Sr. Associate
AnJie Law Firm, China

Email: sunli@anjielaw.com

Phone: +86 21 2422 4979

Mobile: +86 1348 2704 038

Wechat:



Sun Li provides compliance and dispute resolution legal services to a number of world-class companies.

Before she joined AnJie, she has more than 16 years of experience in well-known foreign bank, providing advice and legal analysis for the bank's daily business and governance affairs.

She once served as the General Counsel of a listed company on the New Third Board. She was responsible for building the company's legal team, designing the company's internal control process, HR system and building the risk prevention and control management framework.

ANJIE

安杰律师事务所



Employee Personal Information Processing under the PIPL

December 2021

Content

- Overview of the legal framework for data protection and cybersecurity in China
- Overview of the newly in force Personal Information Protection Law (PIPL)
- Processing employee information – legal rules and practice

Overview of the legal framework for data protection and cybersecurity in China

□ **Laws:**

- Cybersecurity Law (2016)
- Data Security Law (In force on Sept 1, 2021)
- Personal Information Protection Law (In force on Nov 1, 2021)
- Civil Code (2021)
- Criminal Law

□ **Administrative regulations, industry-specific regulations, local administrative regulations**

□ **National standards, industry standards, various best practice guidelines**

Overview of the PIPL

Perhaps the most severe law in China:

- Penalties for Organization: The violator will be ordered to make correction, confiscated of any illegal gains, and fined up to **CNY 50 million (USD 7.8 M)**, or **5%** of last year's annual revenue; and may also be ordered to suspend any related activity or to suspend business for rectification, and/or be reported to the relevant authority for the revocation of the related business permit or the business license.
- Penalties for the person(s) in charge or any other individual directly liable for the violation: They will be fined between **CNY100,000 and CNY1 million (USD 154 K)** and may also be banned for a certain period of time from serving as a director, supervisor, senior officer or personal information protection officer of a relevant enterprise.

Overview of the PIPL



Legal grounds to process personal information under the PIPL

Legal grounds to process personal information

Consent of individuals

The processing is necessary for the conclusion or performance of a contract to which the individual is a party

The processing is necessary for HR management under lawfully formulated employment policies

The processing is necessary to fulfill statutory functions or obligations

The processing is necessary to respond to public health emergencies or protect the life, health or property safety of natural persons under emergency circumstances

Reasonable news/media reporting which is in the public interest

Processing publicly available personal information in a reasonable manner

Other circumstances as provided by law

Understanding “Necessary for HR management according to lawfully formulated employment policies”

To rely on this legal ground to process the personal information of employees, the processing activities need to be:

- necessary
- to conduct human resources management;
- according to lawfully formulated employment policies.

Understanding “Necessary for HR management according to lawfully formulated employment policies”

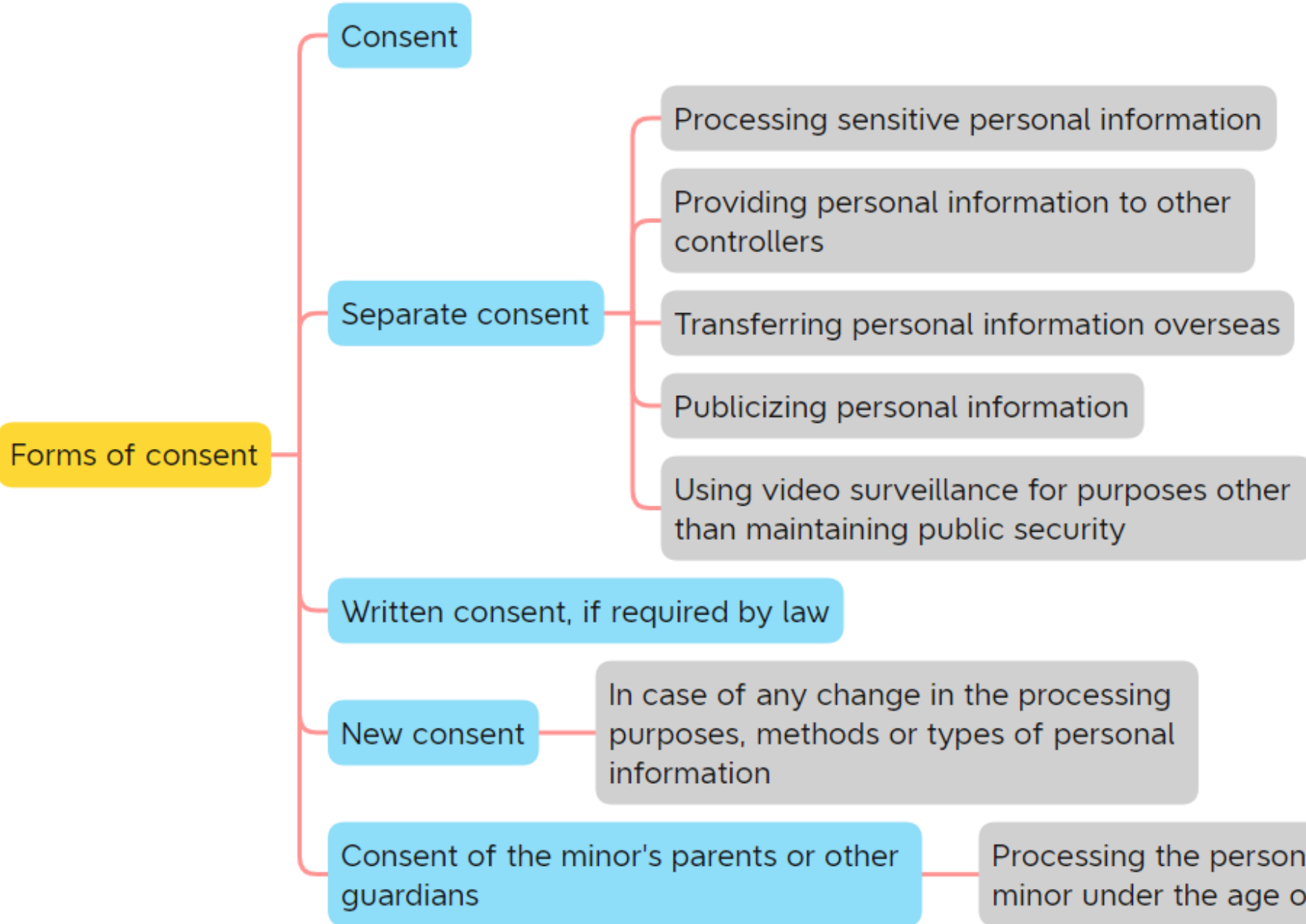
- **“necessary”**: Employers must take into account the development of technologies, social acceptance and durability of the processing activities, and characteristics of the company concerned.
- **“human resources management”**: Employers must differentiate between *“management activities of the HR Department”* and *“human resources management activities of a company”*

Understanding “Necessary for HR management according to lawfully formulated employment policies”

□ “according to lawfully formulated employment policies”:

*Article 4 of the **Labor Contract Law**: ...The formulations, amendments and decisions made by Employers with respect to rules on labor compensation, working hours, leave and rest, occupational safety and hygiene, insurance and welfare, training, work discipline or work quota management, etc., which have a direct impact on employees' immediate rights and interests, or other material matters, **shall be presented to the employee representative congress or all the employees for discussion, and the proposal and advice thereof shall be determined after consultation with the labor union or employee representative on the basis of equality. The Employer shall make rules, regulations and decisions on material matters that have a direct impact on employees' immediate interests and rights, public or communicate the same to the employees.***

Totally relying on the consent of employees would be difficult



*Remember!
Employees can
withdraw their
consent...*

Personal Information Protection Impact Assessment under the PIPL

Personal Information Protection Impact Assessment

Processing of sensitive personal information

Automated decision-making by using personal information

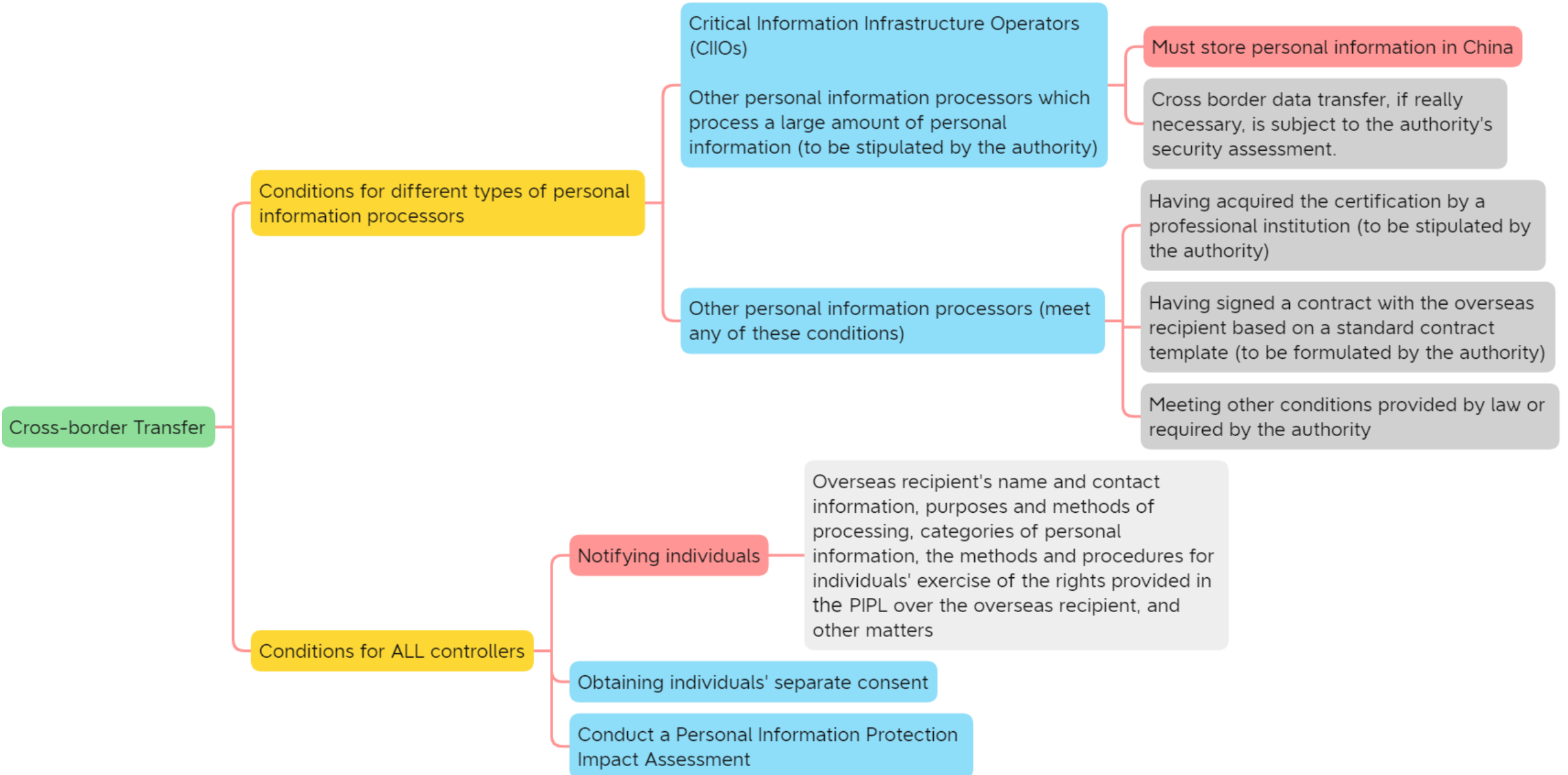
(a) entrusting others to process personal information;
(b) provide personal information to other controllers;
(c) publicize personal information

Transferring personal information overseas

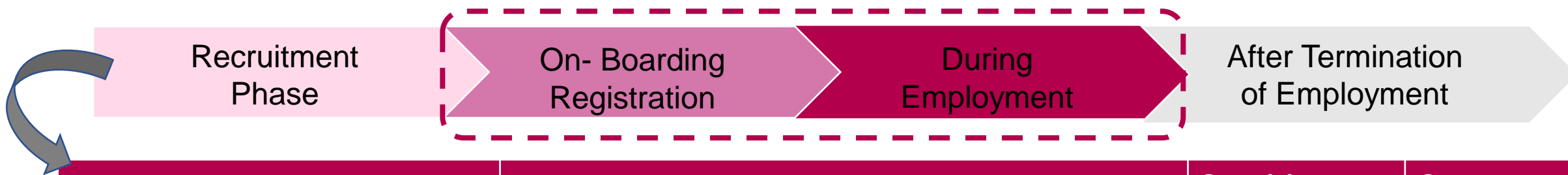
Other processing activities having a material impact on individuals

Keep the assessment reports and processing activity records for no less than 3 years.

Restrictions on cross-border data transfer



Human Resource Management Lifecycle



HR Scenarios	Common Categories of Personal Information*	Sensitive Personal Information	Cross-border transmission
① Receive and check applicant information	① Basic personal information ② Personally identifiable information ③ Personal education and work information	Y	Y/N
② Fill in the application form during written test and interviews	① Basic personal information ② Personal health and physiological information	Y	Y/N
③ Background check	① Education and work history ② Personal property information (credit record) ③ Other information (criminal record)	Y	Y/N

Human Resource Management Lifecycle

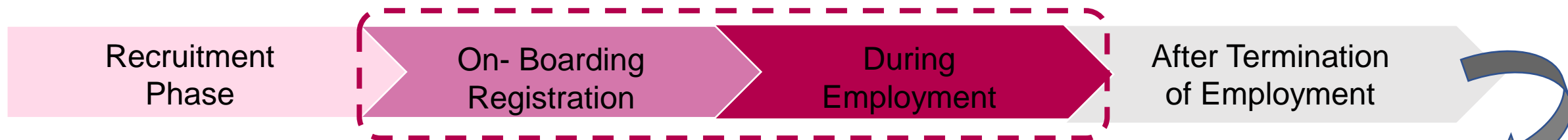


Since candidates are **not** yet on board at the recruitment stage and are **not** bound by an employment contract or the company's HR management policies, Article 13, Item 2 of the PIPL **does not** apply when handling candidates' personal information.

We suggest:

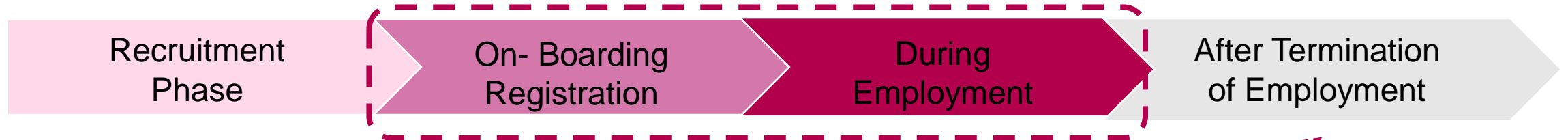
- ① Acquiring consent for the use, storage and cross-border transmission of personal information, and permission for entrusted third parties to process personal information.
- ② Fully reviewing the relevant clauses on personal information protection in service contracts with 3rd parties (recruitment platforms, headhunters, backing agencies, etc.)
- ③ Conducting a personal information protection impact assessment on personal information handling measures as required by the PIPL.

Human Resource Management Lifecycle



HR Scenarios	Common Categories of Personal Information*	Sensitive Personal Information	Cross-border transmission
① Separate employee information	<ul style="list-style-type: none"> ① Personal internet record ② Contact information ③ Personal communication information ④ Personal location information ⑤ Personal common equipment information ⑥ Network identification information 	Y	Y/N
② Employment status during the non-compete period	① Education and work history	Y	Y/N
③ Post-employment background checks	① Education and work history	Y	Y/N

Human Resource Management Lifecycle



Since such individuals are no longer employed by the company and both parties are not bound by the employment contract or the company's HR management policies, Article 13, Item 2 of the PIPL does not apply when handling ex-employee's personal information.

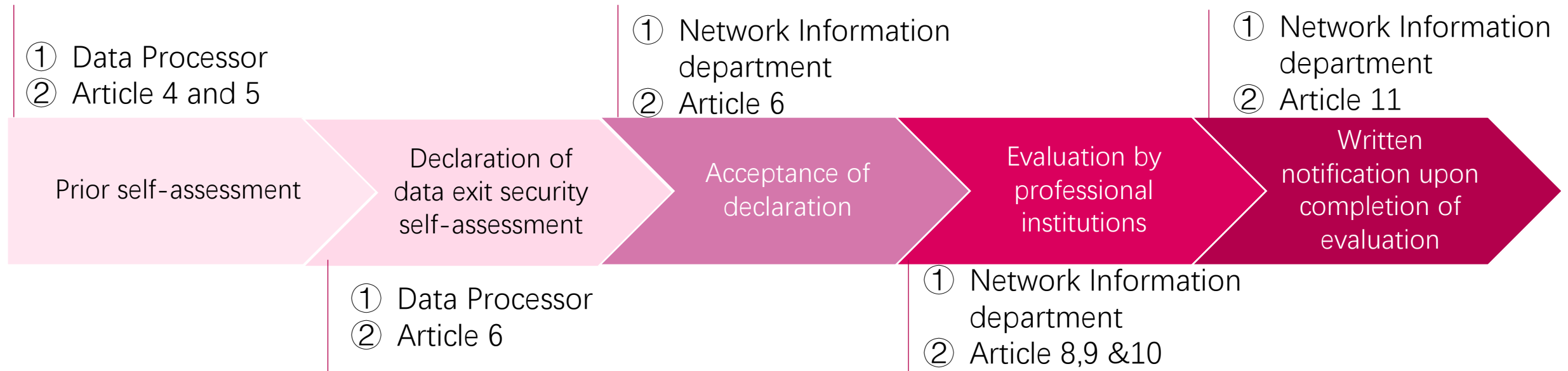
We suggest:

- ① Preparing Termination documents (termination check-list, termination agreement, negotiated release agreement, etc.) that include provisions authorizing the employer to store, use, transmit across borders and allow entrusted third parties to process personal information after termination.
- ② Amending non-compete agreements by adding a right to require individuals to further disclose information and to appoint entrusted third parties to conduct investigations, etc. after termination.
- ③ Improving personal information protection and privacy policies for employees in China subject to the statutory democratic procedures (according to the PIPL, Article 13).
- ④ Conducting personal information protection impact assessment on personal information handling practices as required by the PIPL.

Cross-border transfer of employee data



Measures on Data Exit Security Assessment (Draft)



- Providing abroad any important data collected and generated in their business operation within the PRC and any personal information for which security assessment is required pursuant to the law, data processors shall undergo security assessment in accordance with the provisions herein.
- The security assessment shall adhere to the combination of ex-ante assessment and ongoing supervision, and the combination of internal risk assessment and security assessment, in order to prevent the security risks in cross-border data transfer and guarantee the lawful, orderly and free flow of data.

Article 4

If one of the following circumstances exists, a data exit **security assessment** should be declared to the national cyberspace administration authority through the local provincial cyberspace administration.

- ✓ The personal information and Important Data are and were collected and generated by a Critical Information Infrastructures Operator.
- ✓ The outbound data contains Important Data.
- ✓ The personal information processor has handled the personal information of **at least one million people**.
- ✓ The outbound transfers cumulatively involve the personal information of **over 100,000 people** or the sensitive **personal information of over 10,000 people**.
- ✓ Other situations where the national cyberspace administration authority requires a security assessment exist.

ANJIE

安杰律师事务所

THANKS

杰出 所以安心

DEDICATED
TO EXCELLENCE

BEIJING SHANGHAI HONGKONG SHENZHEN HAIKOU

ANJIELAW.COM