AI Policies and Data Privacy Landscape
The People's Republic of China

Symposium on Data protection in the AI Society

Paula Cao （曹卫红）　　**2019.7.4**

Disclaimer: *The views, thoughts, and opinions expressed in this PPT and during the Symposium on Data Protection in the AI Society on July 4, 2019 by the author belong solely to the author, and not necessarily to the author's employer, organization, committee or other group or individual.*

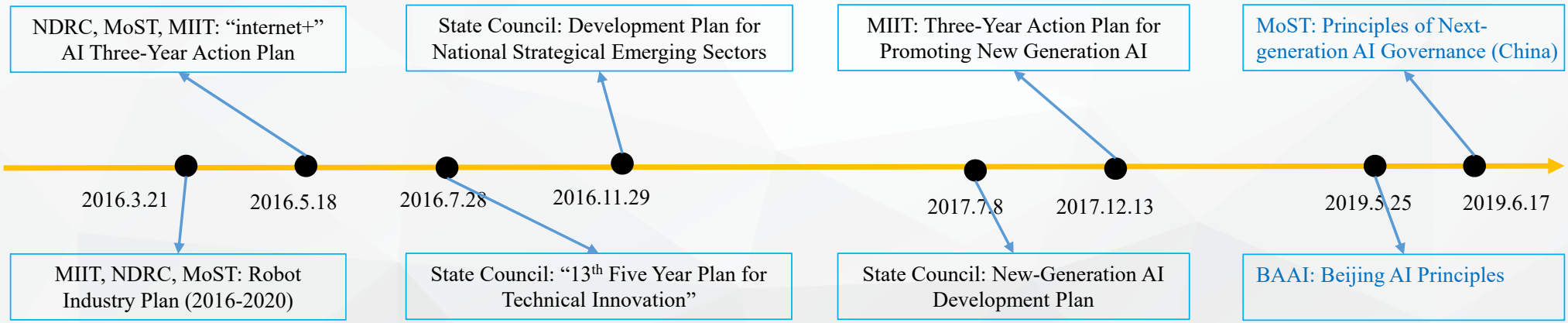
Table of Contents

01 AI Policies in China (Privacy Perspective)

Overview of AI Plan and Policy Development in China

Chinese government was determined to develop AI and released various AI specific plans and policies to guide the development

19th CPC Report → **AI development as a main task** ← **Annual governmental work report 2017/2018/2019**



Beijing AI Principles

The Beijing Academy of Artificial Intelligence (BAAI) released 15 principles in May 2019. It has been proposed as an initiative for the research, development, use, governance and long-term planning of AI.

- **Research and Development**
  1. Do Good
  2. For Humanity
  3. Be Responsible
  4. Control Risks
  5. Be Ethical
  6. Be Diverse and Inclusive
  7. Open and Share

- **Use of AI**
  1. Use Wisely and Properly
  2. Informed-consent
     Ensure stakeholders of AI systems are sufficiently informed of and consented to the impact towards their rights and interests. Reasonable data and service withdrawal mechanisms shall be established to guarantee that users' rights and interests are not compromised.
  3. Education and Training
- **Governance of AI**
  1. Optimizing Employment
  2. Harmony and Cooperation
  3. Adaptation and Moderation
  4. Subdivision and Implementation
  5. Long-term Planning

Principles of Next-generation AI Governance (National Level)

On June 17, A professional committee under China's Ministry of Science and Technology (MoST) has issued eight principles of next-generation artificial intelligence (AI) governance as follows, pledging to develop responsible AI in China.

Eight principles

1. harmony and friendliness
2. fairness and justice
3. inclusiveness and sharing
4. respect for privacy
5. security and controllability
6. shared responsibility
7. open cooperation
8. agile governance

4. Respect for Privacy AI development should respect and protect the privacy of individuals and fully protect an individual's rights to be informed and to choose. Boundaries and rules should be established for the collection, storage, processing and use of personal information. Personal data authorization and withdrawal mechanisms should be improved. Stealing, tampering, leaking and other forms of illegal collection and use of personal information should be strictly prohibited.

02 Overview of Data Protection Rules in China

Data Protection & Cyber Security Rules

- A data protection compliance program needs to include various legal requirements and national standards in China
- The legal framework itself is complex [this is NOT an exhaustive list].

Name	Issuing Authority	Effective Date
1. Laws and Regulations		
National Security Law of the People's Republic of China	Standing Committee of the National People's Congress	2015-7-1
Amendment IX to the Criminal Law of the People's Republic of China (Article 253 The Infringement of Citizen's Personal Information)	Standing Committee of the National People's Congress	2015-11-1
Cyber Security Law of the People's Republic of China	Standing Committee of the National People's Congress	2017-6-1
Resolusion of the Standing Committee of the National People's Congress on Strengthening the Protection of Cyber Information	Standing Committee of the National People's Congress	2012-12-28
National Cyberspace Security Strategy	Cyberspace Administration of China	2016-12-27
International Cooperation Strategy in Cyberspace	Ministry of Foreign Affairs, Cyberspace Administration of China	2017-3-1
Law of the People's Republic of China on the Protection of Consumer Rights and Interests	Standing Committee of the National People's Congress	2014-3-15
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 of Infringing on Citizens' Personal Information	Supreme People's Court, Supreme People's Procuratorate	2017-6-1
Provisions on Protecting the Personal Information of Telecommunications and Internet Users	Ministry of Industry & Information Technology	2013-9-1
2. Administration and Regulations on Contents That Are Posted Online		
Administrative Measures for Internet Information Services (2011 Revision)	State Council	2011-1-8
Provisions on the Administrative Law Enforcement Procedures for Internet Information Content Management	Cyberspace Administration of China	2017-6-1
Provisions for the Administration of Internet News Information Services	Cyberspace Administration of China	2017-6-1
Detailed Rules for the Licensed Management of Internet News Information Services	Cyberspace Administration of China	2017-6-1
Provisions on the Administration of Internet Comments Posting Services	Cyberspace Administration of China	2017-10-1
Provisions on the Administration of Internet Forum and Community Services	Cyberspace Administration of China	2017-10-1
Provisions on the Administration of Internet Group Information Services	Cyberspace Administration of China	2017-10-8
Provisions on the Administration of Internet User Public Account Information Service	Cyberspace Administration of China	2017-10-8

;

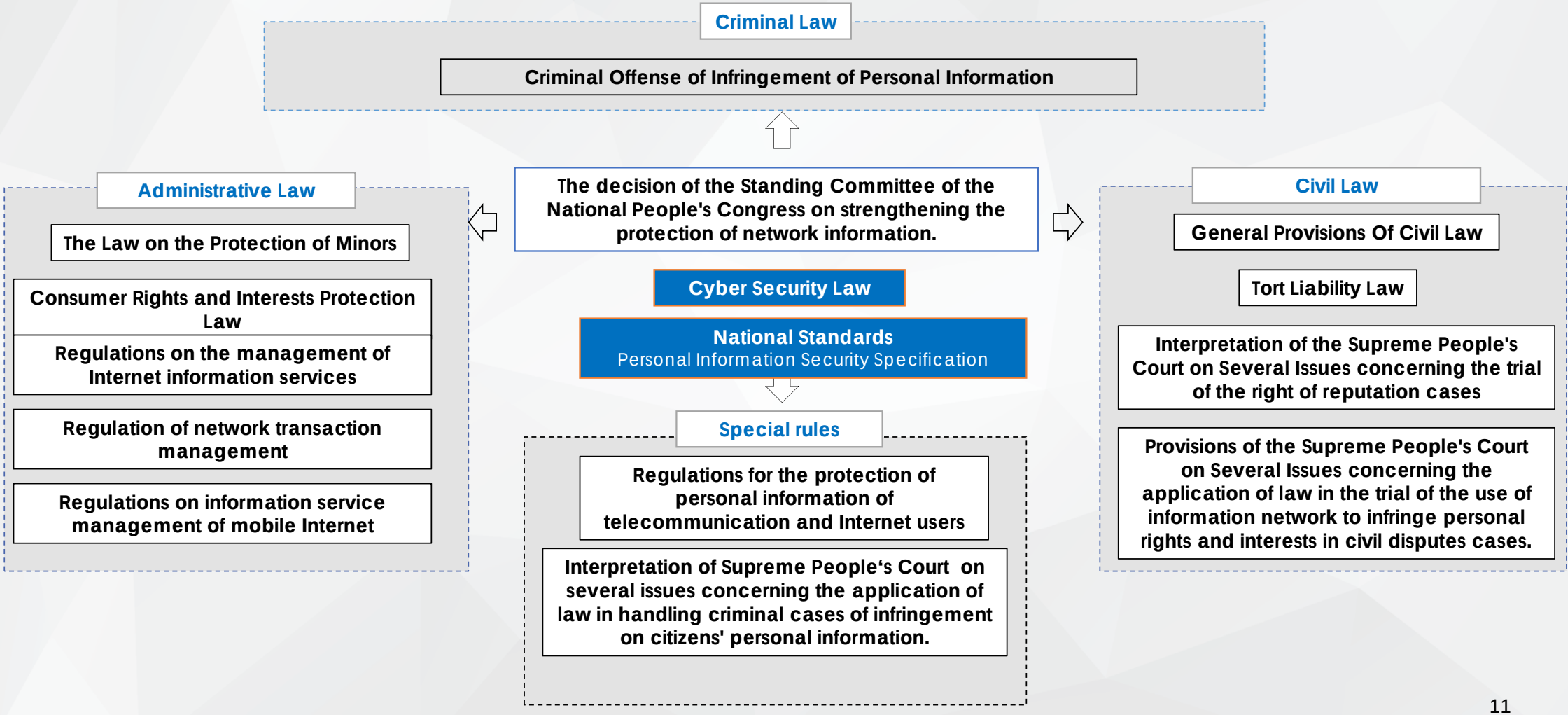
Data Protection & Cyber Security Rules

Name	Issuing Authority	Effective Date
3. Cyberspace Security Graded Protection System		
Information Security Technology: Guidelines for the Implementation of Network Security Grading Protection (Draft for Comments)	National Technical Committee for Standardization of Information Security	N/A
Information Security Technology: Guidelines for the Evaluation Process of Cyberspace Security Grade Protection (Draft for Comments)	National Technical Committee for Standardization of Information Security	N/A
Information Security Technology: Guidelines for the Evaluation Technique of Cyberspace Security Grade Protection (Draft for Comments)	National Technical Committee for Standardization of Information Security	N/A
Information Security Technology: Basic Requirements of Cyberspace Security Grade Protection (Part 1-5) (Draft for Comments)	National Technical Committee for Standardization of Information Security	N/A
Information Security Technology: Design Technical Requirements of Cyberspace Security Grade Protection (Part 1-5)(Draft for Comments)	National Technical Committee for Standardization of Information Security	N/A
Information Security Technology: Evaluation Requirements of Cyberspace Security Grade Protection (Part 1-5) (Draft for Comments)	National Technical Committee for Standardization of Information Security	N/A
4. Cyber Security Requirements on Critical Information Infrastructure Operator		
Regulation for Security Protection of Critical Information Infrastructures (Draft for Comments)	Cyberspace Administration of China	N/A
State Operational Guidelines for Cyberspace Security Check	Office of the Central Network Security and Information Leadership Group, Network Security Coordination Bureau	2016-6
Information Security Technology: Evaluation Guidelines for Security Check of Critical Information Infrastructures (Draft for Comments)	National Technical Committee for Standardization of Information Security	N/A
Information Security Technology: Evaluation Index System for Safety and Security of Critical Information Infrastructures (Draft for Comments)	National Technical Committee for Standardization of Information Security	N/A
Critical Information Infrastructure Identification Guide	Cyberspace Administration of China, Ministry of Industry and Information Technology, Ministry of Public Security, etc.	N/A
Information Security Technology: Cyberspace Protection Requirements of Critical Information Infrastructures	National Technical Committee for Standardization of Information Security	N/A

Data Protection & Cyber Security Rules

Name	Issuing Authority	Effective Date
5. Protection System for Personal information and Important Data		
Assessment Guidelines for Personal information and Important Data Exit (Draft for Comments and Revision)	Cyberspace Administration of China	N/A
Information Security Technology: Security Assessment Guidelines for Data Exit (Draft for Comments)>	National Technical Committee for Standardization of Information Security	N/A
Information Security Technology: Standard for Personal Information Security	National Technical Committee for Standardization of Information Security	2019-6-25
Information Security Technology: Guidelines for De-identification of Personal Information (Draft for Comments)	National Technical Committee for Standardization of Information Security	N/A
Information Security Technology: Guidelines for the Protection of Personal Information in Public and Commercial Service Information Systems	Ministry of Industry and Information Technology	2013-2-1
6. The Administrative System for Network Products and Service		
Measures for the Security Review of Network Products and Services (for Trial Implementation)	Cyberspace Administration of China	2017-6-1
Information Security Technology: General Requirements for Network Product and Service Security (Draft for Comments)	National Technical Committee for Standardization of Information Security	N/A
Information Security Technology: The Conditions and Code of Conduct of the Information Technology Product Safety Inspection Agency (Draft for Comments)	National Technical Committee for Standardization of Information Security	N/A
Information Security Technology: Controllable Evaluation Index for Information Technology Product Safety (part 1-5)(Draft for Comments)	National Technical Committee for Standardization of Information Security	N/A
7. The Administrative System for Network Security Incidents		
National Emergency Plan for Network Security Incidents	Office of the Central Network Security and Information Leadership Group	2017-1-10
Guidelines for Emergency Management of Information Security Incidents in Industrial Control Systems	Ministry of Industry and Information Technology	2017-5-31
Information Security Technology: Definition and Description Specification for Network Attack (Draft for Comments)	National Technical Committee for Standardization of Information Security	N/A
Information Security Technology: General Guidelines for Emergency Rehearsal of Network Security Incidents (Draft for Comments)	National Technical Committee for Standardization of Information Security	N/A

Main Data Protection Rules in China



03 Key Points of Chinese Data Protection Rules

Data Protection Basic Principles: GDPR vs Chinese Rules

Processing of personal data must be **fairly**, **lawfully** and **transparently**

Processing of personal data must be **adequate**, **relevant and not excessive**

Processing of personal data must be for **limited purposes**

Accurate and, where necessary, kept up to date

Personal data shall be kept **for a period no longer than is necessary** for the purposes for which the data was collected

Accountability (key difference between GDPR and China laws): data controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate the compliance with GDPR. Chinse laws does not have this principle.

Lawful Basis: GDPR vs Chinese Rules

- Consent
- Performance of Contract
- Compliance with law
- Protection of Vital Interest
- Public Interest
- Legitimate Interest

GDPR

- Consent
- Performance of Contract
- Compliance with law
- Protection of Vital Interest
- Public Interest
- ~~Legitimate Interest~~

Chinese Law or National Standard

Data Subject Rights: GDPR vs Chinese Rules

- Right to be informed
- Right to access
- Right to amend, correct /update
- Right to data portability

- Right to deletion

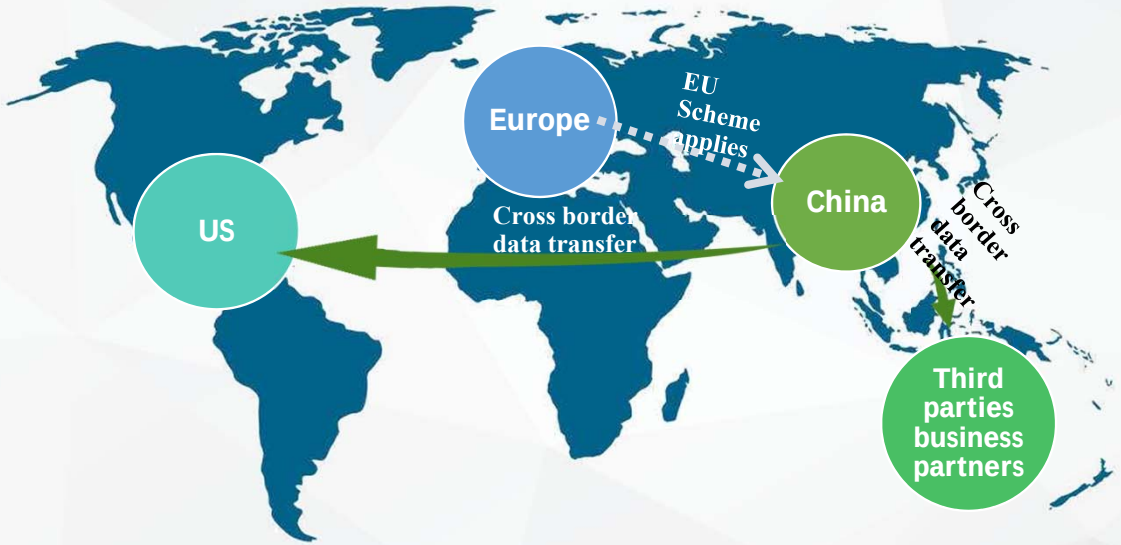
- Right to restriction of processing (Article 18)
- Right to withdraw consent
- Right to opt-out of marketing communications
- Right not to be subject to fully automated decisions

GDPR

- Right to be informed
- Right to access
- Right to amend, correct /update
- Right to data portability
  a) Basic personal materials, personal ID data
  b) Personal health/biometric data, personal education/job data
- Right to deletion
  - Breach law or agreement
  - After accounts de-registration
- N/A
- Right to withdraw consent
- Right to opt-out of marketing communications
- Right not to be subject to fully automated decisions

Chinese Law or National Standard

International Data Transfer Scheme in China



On cross-border data transfer, the scheme in China would likely to be more stringent than the scheme in the EU. Pursuant to the Cybersecurity Law Personal data and important data of Critical Information Infrastructure operators (CIIO) shall not be provided to individuals or organizations outside China without approval.

Draft Measures on Security Assessment of the Cross-border Transfer of Personal Information (June 13)

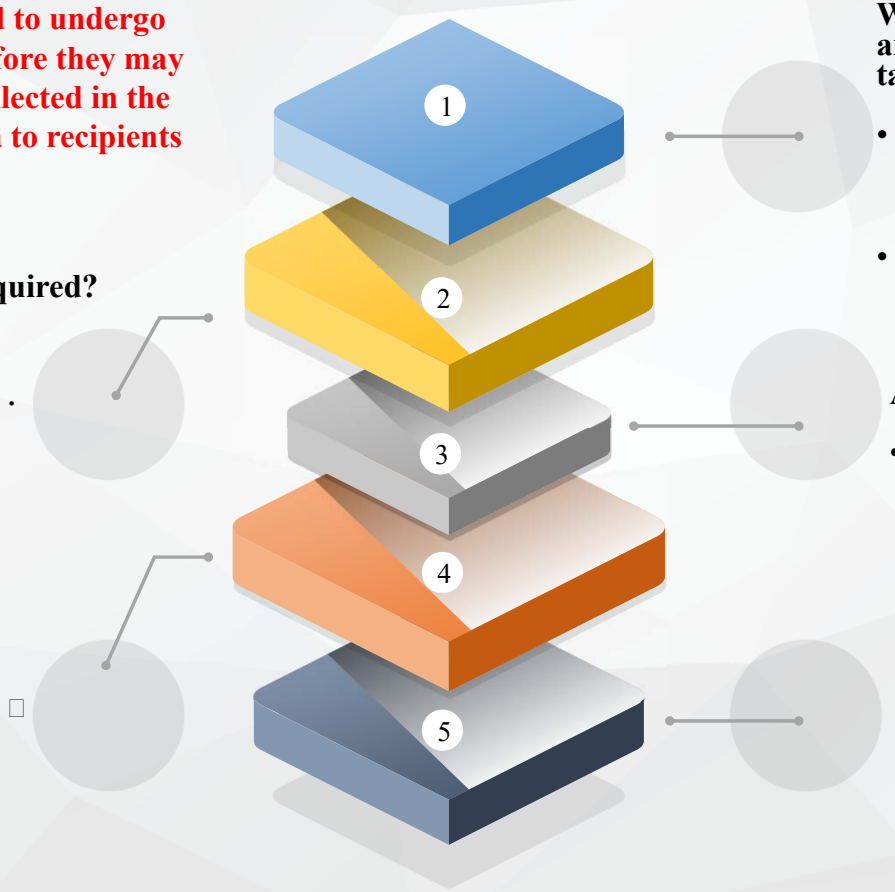
All network operators are obliged to undergo the security assessment process before they may transfer personal information collected in the course of their operations in China to recipients outside China.

When the security assessment will be required?

- Before transfer

Materials must be submitted for the assessment:

- the application letter;
- the contract between the network operator and the recipient;
- the security assessment report on the security risks and the adopted security measures; and
- other materials required by the CAC.



Who will conduct the security assessment and how long will the assessment process take?

- After the Provincial CAC has received all the required application materials, it will organize experts to carry out the security assessment
- within 15 business days or longer under complex situations

Annual Report required

- Network operators must submit annual reports to their local cyberspace administration authority;

Security incident notification

- If a "relatively serious" security incident occurs, the network operator must report it to the Provincial CAC in a timely manner.

Legal Ramifications: Administrative Liability

	GDPR Article 83 (4)	GDPR Article 83 (5)
Cap on Penalty	An individual：10 million Euro An undertaking：10 million Euro or 2% of total worldwide annual turnover in preceding year for undertakings (the higher of the two)	An individual：20 million Euro An undertaking：20 million Euro or 4% of total worldwide annual turnover in preceding year for undertakings (the higher of the two)
Applicability	Covers issues such as children consent, data protection by design and by default, engagement of processors by controllers, records of processing, cooperation with regulators, security, breach notification, data protection impact assessment, DPOs, code of conduct and certification	Covers issues such as data protection principles, lawfulness of processing, consent, processing of special category of data, the data subject's rights, international transfers, failure to comply with the supervisory authority's investigatory and corrective powers.

Article 64 of China Cyber Security Law:

- Rectification order
- Written warning
- Confiscation of illegal gain
- 1 to 10 times of illegal gain as fine
- Up to RMB1 million as fine in the absence of illegal gain
- Fine on direct responsible management personnel at RMB10k to RMB100k
- In the case of severe violation, suspension of relevant business, rectification, cessation of website, revocation of permit or business license

Criminal Liability

Illegal act	Serious Circumstances	Liability
Obtain; Steal; Sell; Provide; or Publish online Personal info of citizens	For Example: (1) selling or providing information on whereabouts and used by others for crime; (2) acknowledging others have used personal information to commit crimes and still sell or provide it to them; (3) illegally obtaining, selling or providing information on whereabouts, communication content, credit information, and property of more than 50 pieces; (4) illegally obtaining, selling or providing information on accommodation, communication records, health, transaction and other information of more than 500 citizens; (5) illegally obtaining, selling or providing more than 5,000 personal information other than that specified in Item 3 and 4; (6) the respective amount of certain information does not reach the criteria, but the amount in aggregate surpasses the stipulated threshold.; (7) The illegal income is more than 5,000 RMB; (8) Selling or providing personal information obtained in the course of performing duties or providing service, and the quantity of information or the amount of illegal gains is higher than half of the threshold specified in Item 3-7; (9) having been criminally punished for infringing personal information or having received administrative punishment within two years, and illegally obtaining, selling or providing personal information of the citizen again; (10) other serious circumstances.	• Imprisonment less than 3 years; • Criminal detention in addition to a fine; or • a fine only.
	Particularly Serious Case: (1) resulting in death, serious injury, psychiatric disorder of the victim, or that the victim is kidnapped, or causing any other serious consequence; (2) leading to major economic losses or evil social influences; (3) quantity of information or the amount of illegal gains is over ten times as much as the criteria specified in Item 3-8 of the preceding paragraph; (4) any other circumstance where the case is particularly serious.	• Imprisonment 3-7 years in addition to a fine

THANKS