ASIA-PACIFIC CSD GROUP

中国结算 CSDC

China Securities Depository and Clearing Corporation Limited

Legal Task Force Group Meeting

Data Security and Governance

Shuqing Wang,

Legal Affairs Department, CSDC

shuqingwang@chinaclear.com.cn

November, 2022

CONTENTS

/01

Data and Bigdata in Legal Perspective

01 Data and Bigdata in Legal Perspective

How to define *data* and *bigdata*?

DATA

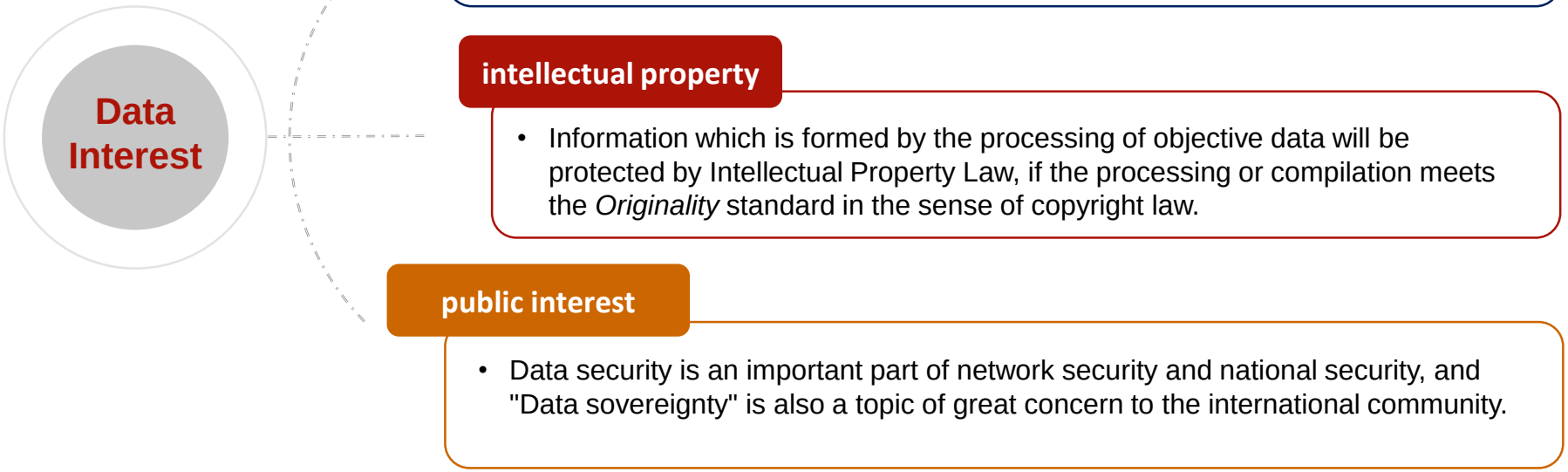
- Data is generally understood as a set of symbols representing objective facts, which can be numbers, characters, words, etc.

BIGDATA

- Gartner Glossary: bigdata is high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation.

01 Data and Database in Legal Perspective

How to protect data-related interest ?



/02

Brief Introduction of Important Data Legislation

02 Brief Introduction of Important Data Legislation

Important data legislation in United States

Laws and Acts	Purpose
Clarifying Lawful Overseas Use of Data Act	Extraterritorial jurisdiction of data
National Security and Personal Data Protection Act of 2019 (proposal)	To limit cross-border transfer of data in specific counties
Children's Online Privacy Protection Act	Provide data protection requirements for children's information collected by online operators
Communications Act of 1934	Include data protection provisions for common carriers, cable operators, and satellite carriers
Consumer Financial Protection Act	Regulates unfair, deceptive, or abusive acts in connection with consumer financial products or services.
Federal Securities Law	May require data security controls and data breach reporting responsibilities

- There is no uniform data protection legislation at the federal level in the United States, while the laws in the single industry of finance, telecommunications, education, health care set up data security-related provisions. In the area of data cross-border activity, the United States has enacted the CLOUD ACT and the NSPDPA Act.

ASIA-PACIFIC CSD GROUP

中国结算 CSDC

02 Brief Introduction of Important Data Legislation

Important data legislation in United States

Acts in the field of data cross-border transfer

The CLOUD Act

- ***Clarifying Lawful Overseas Use of Data Act***

- "A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record or other information is located within or outside of the United States."

NSPDPA (proposal)

- ***National Security and Personal Data Protection Act of 2019***

- Intended to prohibits the transfer of data to, and storage of data within, foreign countries that threaten U.S. national security.
- NSPDPA explicitly locks its regulatory targets into certain "Covered Technology companies," The identification of these companies will be determined (or removed) by a process established by the Secretary of State after the passage of the act.

ASIA-PACIFIC CSD GROUP

中国结算 CSDC

02 Brief Introduction of Important Data Legislation

☐ Important data legislation in the European Union: GDPR

General Data Protection Regulations (GDPR)

Since 1970s, the EU countries started domestic data security legislation, and the famous Convention No.108 was published by the Council of Europe in 1981.

- **The "strictest ever" personal data protection regulation**
  - GDPR was published in 2016
  - Generally, as long as the data controlled, processed and monitored by the enterprise involves the personal data of the EU member states, it shall be subject to the GDPR

- **The cross-border transmission of data: Chapter 5**
  - "Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organization shall take place only if, subject to the other provisions of this Regulation. "

ASIA-PACIFIC CSD GROUP

中国结算 CSDC

02 Brief Introduction of Important Data Legislation

Important data legislation in the European Union: PFFND

European Union Regulation on the Free Flow of Non-personal Data (PFFND)

- Aim: to lift main obstacles of data's free flow and to boost the data economy through facilitating cross-border exchange of data by enabling companies to store non-personal information anywhere in the EU.
- Non-personal data: electronic information that cannot be traced back to an identified or identifiable natural person (or has been anonymized as such). Specific examples of non-personal data include aggregate and anonymized datasets used for big data analytics, data on precision farming that can help to monitor and optimize the use of pesticides and water or data on maintenance needs for industrial machines.

02 Brief Introduction of Important Data Legislation

☐ Important data legislation in Asia-Pacific region: CBPR

APEC Cross-border Privacy Rules (CBPR)

- The APEC Privacy Framework 2005: laid out a set of nine principles to assist APEC economies in developing data privacy approaches that optimize privacy protection and cross-border data flows
- CBPR 2011: aims at improving the free flow of personal information and protect data privacy in APEC economies to facilitate the cross-border transfer of personal data between companies in APEC members

☐ The CBPR System protects personal data by requiring:

- **Enforceable standards**
- **Risk-based protections**
- **Consumer empowerment**
- **Cross-border enforcement cooperation**
- **Accountability**
- **Consumer-friendly complaint handling**
- **Consistent protections**

ASIA-PACIFIC CSD GROUP

中国结算 CSDC

02 Brief Introduction of Important Data Legislation

☐ Important data legislation in Asia-Pacific region: CBPR

APEC Cross-border Privacy Rules (CBPR)

☐ The CBPR System protects personal data by requiring:

- **Enforceable standards**: To join, participating economies must demonstrate that CBPR program requirements will be legally enforceable against certified companies.
- **Accountability:** To become certified, a company must demonstrate to an Accountability Agent—an independent CBPR System-recognized public or private sector entity— that they meet the CBPR program requirements, and the company is subject to ongoing monitoring and enforcement.
- **Risk-based protections:** Certified companies must implement security safeguards for personal data that are proportional to the probability and severity of the harm threatened, the confidential nature or sensitivity of the information, and the context in which it is held.
- **Consumer-friendly complaint handling:** Accountability Agents receive and investigate complaints and resolve disputes between consumers and certified companies in relation to non-compliance with its program requirements.
- **Consumer empowerment:** Certified companies must provide consumers with the opportunity to access and correct their personal data. Further, by publicly certifying to the CBPR System's requirements, consumers gain insight into the privacy practices on business with which they choose to do business.
- **Consistent protections:** While governments may impose additional requirements with which certified companies must still comply, all participants must agree to abide by the 50 CBPR program requirements, facilitating the implementation of the same baseline protections across different legal regimes.
- **Cross-border enforcement cooperation:** The CBPR System provides a mechanism for regulatory authorities to cooperate on the enforcement of program requirements.

/03

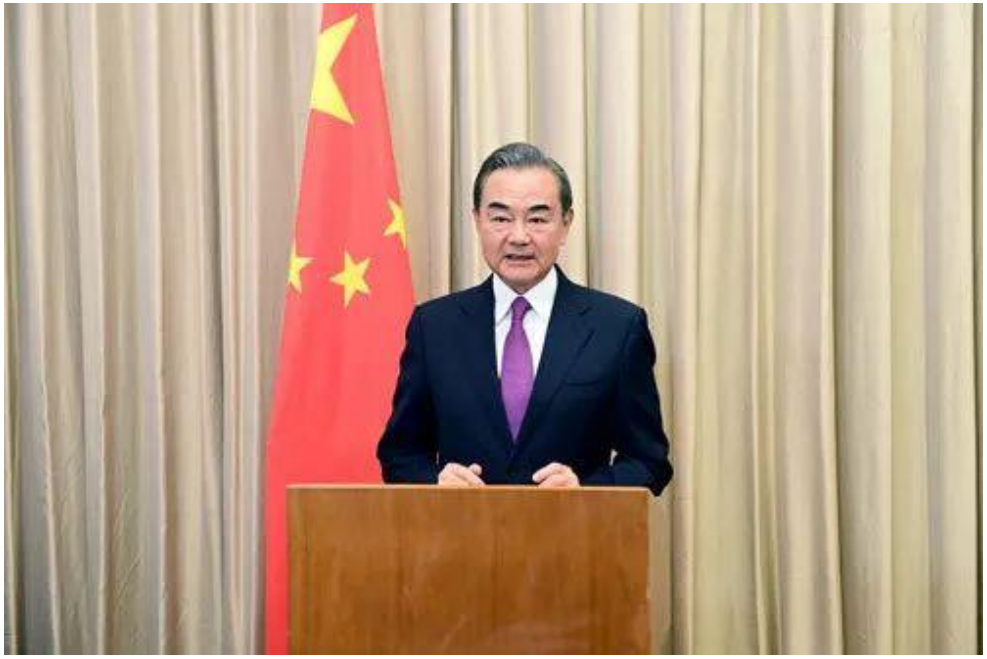
Global Initiative on Data Security

03 Global Initiative on Data Security

Global Initiative on Data Security

- On September 8,2020, the international Seminar on Global Digital Governance with the theme of "Seizing Digital Opportunities for Cooperation and Development“ was held in Beijing.

- At the meeting, State Councilor and Foreign Minister of China, Wang Yi proposed the Global Data Security Initiative.



ASIA-PACIFIC CSD GROUP

中国结算 CSDC

Global Initiative on Data Security

- The phenomenal development of information technology revolution and digital economy is transforming the way of production and life, exerting far-reaching influence over social and economic development of States, global governance system and human civilization.
- The explosive growth and aggregation of data, as a key element of digital technology, has played a crucial role in facilitating innovative development and reshaping people's lives, bearing on security and economic and social development of States.
- In the context of closer global cooperation and new development of international division of labor, maintaining supply chain security of ICT products and services has never become more important for boosting users' confidence, ensuring data security and promoting digital economy.
- We call on all States to put equal emphasis on development and security, and take a balanced approach to technological progress, economic development and protection of national security and public interests.

Global Initiative on Data Security

- We reaffirm that States should foster an open, fair and non-discriminatory business environment for mutual benefit, win-win outcomes and common development. At the same time, States have the responsibility and right to ensure the security of important data and personal information bearing on their national security, public security, economic security and social stability.
- We welcome governments, international organizations, ICT companies, technology communities, civil organizations, individuals and all other actors to make concerted efforts to promote data security under the principle of extensive consultation, joint contribution and shared benefits.
- We underscore that all parties should step up dialogue and cooperation on the basis of mutual respect, and join hands to forge a community with a shared future in cyberspace featuring peace, security, openness, cooperation and order. To make this happen, we would like to suggest the following:

03 Global Initiative on Data Security

Global Initiative on Data Security

- ✓ States should handle data security in a comprehensive, objective and evidence-based manner, and maintain an open, secure and stable supply chain of global ICT products and services.
- ✓ States should stand against ICT activities that impair or steal important data of other States' critical infrastructure, or use the data to conduct activities that undermine other States' national security and public interests.
- ✓ States should take actions to prevent and put an end to activities that jeopardize personal information through the use of ICTs, and oppose mass surveillance against other States and unauthorized collection of personal information of other States with ICTs as a tool.
- ✓ States should encourage companies to abide by laws and regulations of the State where they operate. States should not request domestic companies to store data generated and obtained overseas in their own territory.
- ✓ States should respect the sovereignty, jurisdiction and governance of data of other States, and shall not obtain data located in other States through companies or individuals without other States' permission.

03 Global Initiative on Data Security

Global Initiative on Data Security

- ✓ Should States need to obtain overseas data out of law enforcement requirement such as combating crimes, they should do it through judicial assistance or other relevant multilateral and bilateral agreements. Any bilateral data access agreement between two States should not infringe upon the judicial sovereignty and data security of a third State.
- ✓ ICT products and services providers should not install backdoors in their products and services to illegally obtain users' data, control or manipulate users' systems and devices.
- ✓ ICT companies should not seek illegitimate interests by taking advantage of users' dependence on their products, nor force users to upgrade their systems and devices. Products providers should make a commitment to notifying their cooperation partners and users of serious vulnerabilities in their products in a timely fashion and offering remedies.
- We call on all States to support this initiative, and confirm the aforementioned commitments through bilateral, regional and international agreements. We also welcome global ICT companies to support this initiative.

Thank you!

China Securities Depository and Clearing Corporation Limited (CSDC)

Address: No. 17 Taipingqiao Street, Xicheng District, Beijing

www.chinaclear.cn