WIKBORG | REIN
100 YEARS YOUNG

Cybersecurity update

Bård Breda Bjerken and Sherry Qiu

27 August 2024

Agenda

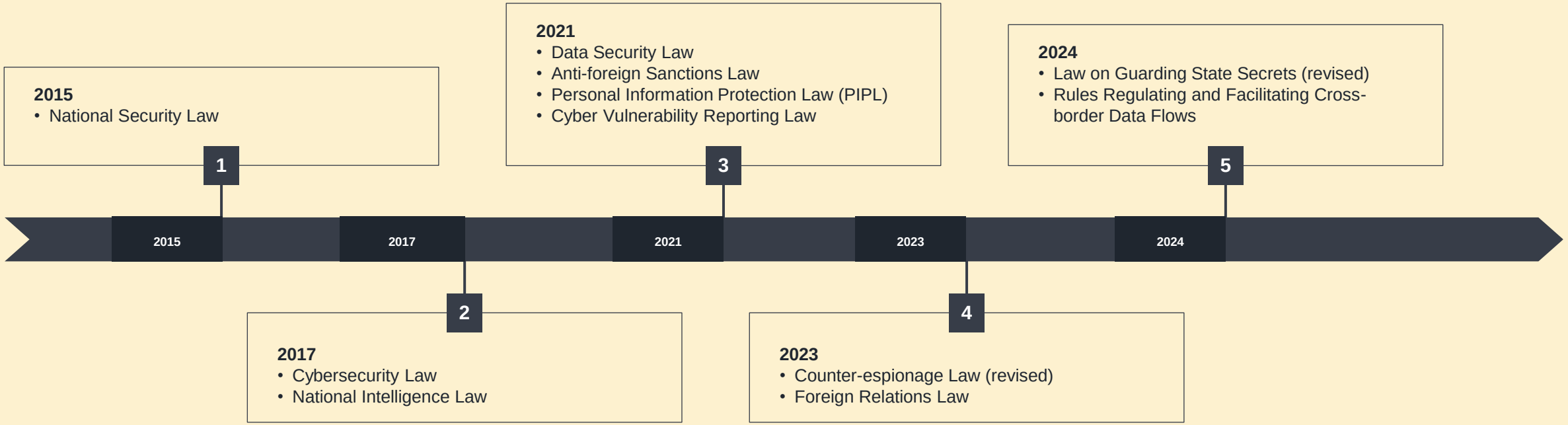
- Legal framework
- Data protection and cybersecurity
- Security regulations

1.

Legal framework

Overview of the regulatory landscape

Key developments



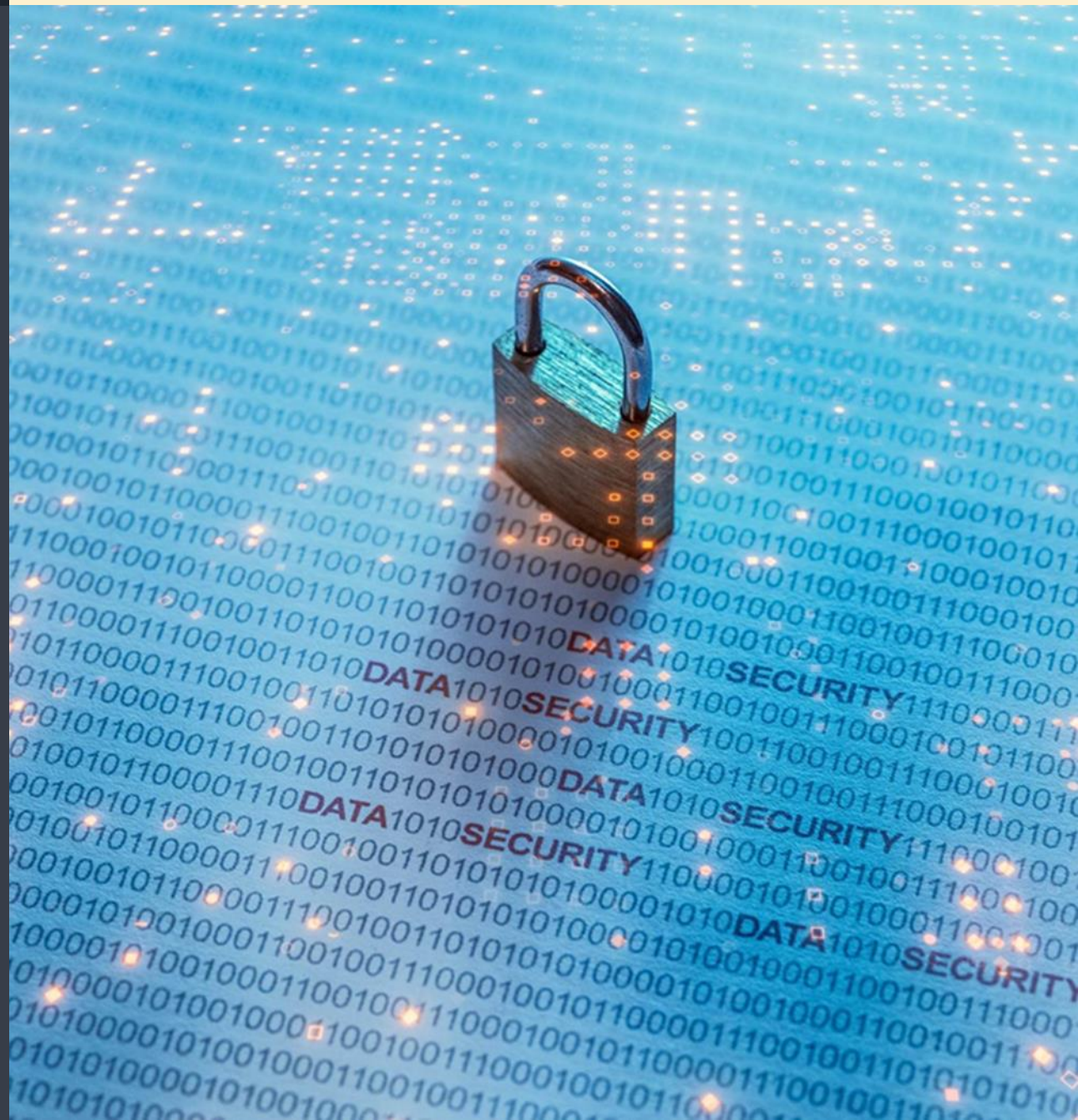
The three pillars

- Cybersecurity law (2017) – critical infrastructure data
  - Overall security framework
  - Mandates that critical infrastructure companies retain their data within China's borders
- Data security law (2021) – cross-border data flows
  - Protection of processed data
  - Subjects cross-border data flows to additional regulatory requirements and prohibitions
- PIPL (2021) – personal data
  - Personal information protection
  - Codifies the privacy rights of PRC citizens

2.

Data protection and cybersecurity

Key obligations for foreign businesses



Cybersecurity law (2017)

- Purpose
  - Safeguards cybersecurity and cyberspace sovereignty
  - Protects national security and the interest of citizens and organisations
- Network operators
  - Network owners, managers, and network service providers
  - Additional security responsibilities
- Critical information infrastructure operators (CIIO)
  - Operators of information systems in important industries and fields
- Enforcement
  - Fines, suspension of business activities and revocation of licenses
- Regulation on protection of security of critical information infrastructure (2021)
  - Security reviews and assessments
  - Data localization requirements
  - Restrictions on cross-border data flows
- Multi-level protection scheme (MLPS)
  - Technology standard and risk based classification based on 5 levels
  - Certification and third-party audits

Data security law (2021)

- Framework for classifying data collected and stored in China
  - Core data
  - Important data
- Applies to data handling activities carried out within the territory of the People's Republic of China by any person or entity
- Restrictions on cross-border transfer of data
- Establishment of an emergency response mechanism for data security
- Personal information
  - Internal data security management
  - Training
  - Security measures
  - MLPS compliance
  - Handle security vulnerabilities and incidents
- Important data
  - Security assessments and reviews
  - Filing requirements
  - Designation of responsible person

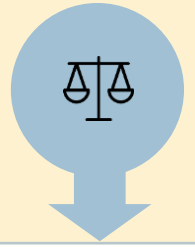
PIPL (2021)

- Codifies the privacy rights of PRC citizens
  - Processing of personal information carried out in China
  - Processing of personal information of any person in China carried out **outside of China** if the purpose is:
    - To provide a **product or service** to person in China;
    - To **analyse or assess the behaviour** of a person located in China; or
    - Any other circumstance as provided by law
- Requires domestic and foreign companies to comply with reviews
  - Controls handling of personal data within and outside mainland PRC when providing products or services to persons within the PRC
  - Restricts ability of companies in China to gather and retain personal data
  - Authorizes the PRC government to collect personal data for actions deemed to be in the public interest
- Sanctions
  - Fines up to **RMB 50 million** or **5%** of the personal information processor's **turnover** the last year
  - Other sanctions include the typical Chinese sanctions for breach of laws:
    - Revoking business license and permits
    - Rectification
    - Confiscation of gains, and
    - Key personnel being held liable

"***PERSONAL INFORMATION*** *refers to any kind of information* ***related to an identified*** *or* ***identifiable natural person*** *as electronically or otherwise recorded, excluding information that has been anonymized*"

"***PROCESSING*** *of personal information includes the* ***collection, storage, use, processing, transmission, provision, disclosure****, and* ***deletion*** *of personal information*"

PIPL (2021) – Key issues to be aware of



GENERAL PRINCIPLES FOR PROCESSING (Art. 5)

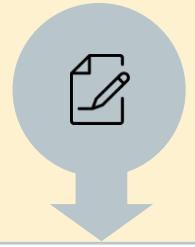
- Must adhere to the principles of
  - **lawfulness**
  - **legitimacy**
  - **necessity**
  - **good faith**
- Not be misleading, fraudulent or coercive

PURPOSE AND SCOPE OF PROCESSING (Art. 6)

- For a **specified, reasonable and direct purpose**
- To be conducted in a way that has the **least impact** on personal rights and interests
- Minimum scope and not excessive collection

PROCESSOR'S RESPONSIBILITIES AND STRUCTURE (Art. 9, 20, 21)

- **Responsible** for processing activities
- Must take **necessary measures to ensure the security** of the personal information
- **Joint processors** to agree on purpose and method as they are joint and severally liable
- **Entrusted processor** requires supervising and compliance



LEGAL BASIS FOR PROCESSING PERSONAL INFORMATION (Art. 13)

- Personal consent unless:
  - Needed to conclude or **perform contractual obligations**;
  - **HR management** employment policy, collective employment contract;
  - Personal information already **disclosed by the individual** or otherwise legally disclosed within a reasonable scope; or
  - Performance of **legal duties**, etc.

SEPARATE / EXPLICIT CONSENT REQUIRED FROM INDIVIDUALS (Art. 23, 25, 29, 39)

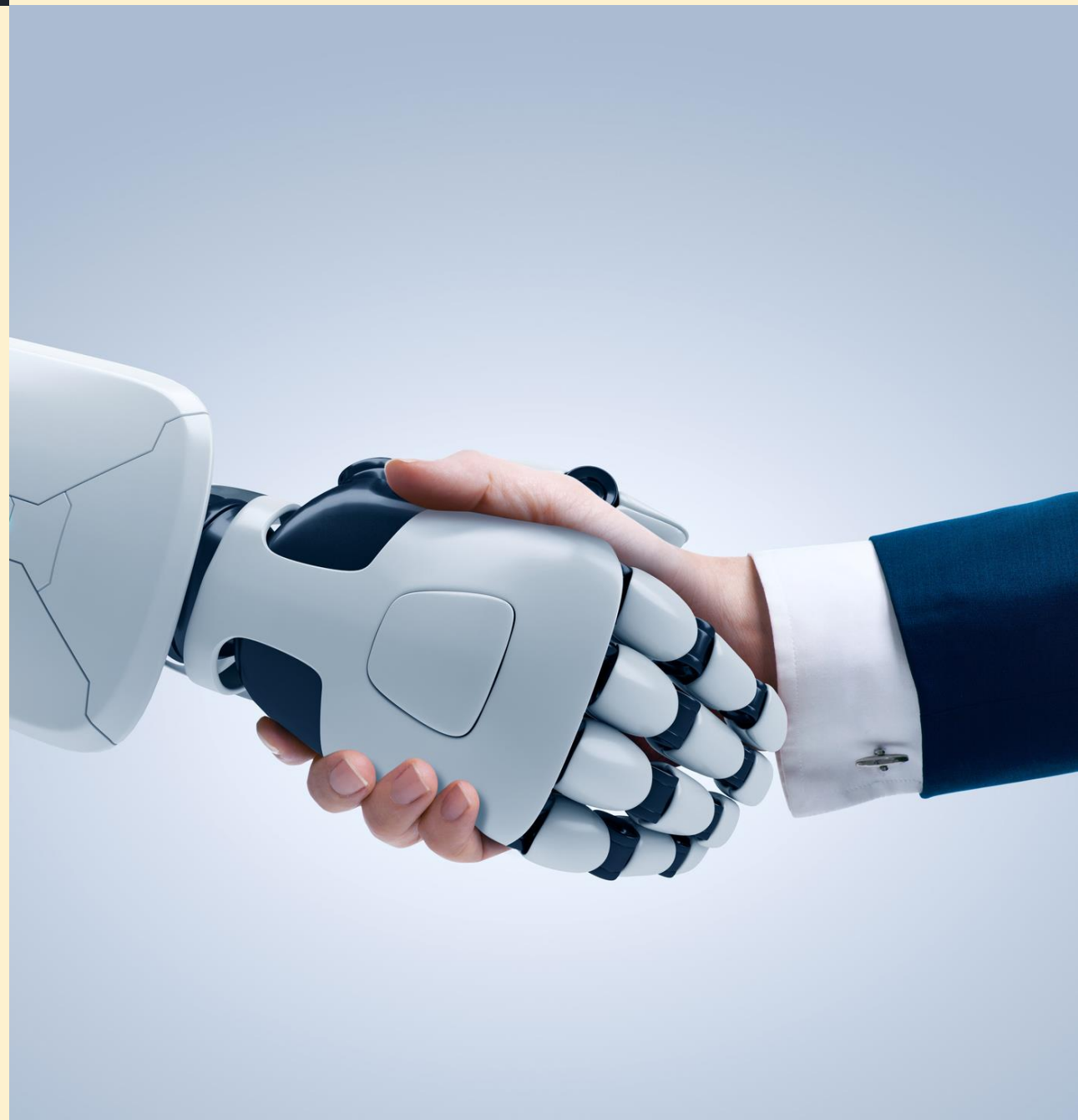
- Providing **to a third party**
- Disclosure **to the public**
- Use of any personal image/ identification information other than for maintaining public security
- Processing of **sensitive personal information**
- **Cross-border transfer**

INDIVIDUALS' REQUEST TO EXERCISE THEIR RIGHTS (Art. 50)

- The individuals have the right to request the processor to **explain the processing of personal information rules** to them
- The individuals can initiate **lawsuits** against the processor if their request to exercise their rights is denied

PIPL (2021) – Consent

- Personal consent must be
  - A voluntary and explicit indication of intent; and
  - Given by the individual on a fully informed basis
- Personal consent must be obtained **again** if
  - Change of purpose or method of processing; or
  - Change in type of personal information to be processed
- Processors cannot refuse to provide the product/ service to the individual if consent is not obtained (or later withdrawn), unless the processing of personal information is necessary to provide the product/service



2024 updates

- Rules Regulating and Facilitating Cross-border Data Flows came into effect on 22 March 2024
  - Exemptions for filing of standard contract, security assessment and personal information protection certification
  - The role of Free-Trade Zones in facilitating data exit is further clarified
  - Simplified filing requirements
- Basic Security Requirements for Generative AI Service (draft issued for comments)
  - Specific security guidance for generative AI services
- Administrative Measures for the Reporting of Cybersecurity Incidents (draft issued for comments)
  - Reporting obligations of network operators on Cybersecurity Incidents

Rules Regulating and Facilitating Cross-border Data Flows

- Exemption for filing of standard contract, security assessment and personal information protection certification
  - Outbound transfer personal information (excluding important data)
    - Data subject is party to an international contract
    - Cross-border HR management
    - Emergency situations for protection of life or property
    - **Quantitative exemptions** for common cross-border transfers below 100,000 per year
  - Outbound transfer of data (excluding important data and personal information) generated during international trade, cross-border transportation, academic cooperation, and transnational production, manufacturing, and marketing activities
  - Outbound transfer of personal information (excluding important data and personal information from China) collected and generated overseas by data processors

Rules Regulating and Facilitating Cross-border Data Flows

- Requirements for cross-border transfer of sensitive personal information
  - **Security assessment**: more than 10,000 people since 1st of January in the current year
  - **Filing of standard contract**: less than 10,000 people since 1st of January in the current year
- When security assessment is required
  - CIIO cross-border transfer of data
  - Non-CIIO cross-border transfer of personal information of **more than 1 million** since 1st of January in the current year
  - Non-CIIO cross-border transfer of sensitive personal information of **more than 10,000** since 1st of January in the current year
  - Non-CIIO cross-border transfer of any important data
- When filing of standard contract or personal information protection certification is required:
  - Non CIIO cross-border transfer of personal information of **more than 100,000** and **less than 1 million**;
  - Non CIIO cross-border transfer of sensitive personal information of **less than 10,000** since 1st of January at the current year.

3.

Security regulations

Changes to be aware of

Foreign relations law (2023)

- Comprehensive framework for China's foreign relations
- Aim to "*safeguard China's national sovereignty, national security and development interests and uphold international fairness and justice*"
- Has counter and restrictive measures in defence against extraterritorial application of foreign laws, as well as actions that are "*detrimental to China's national interests*"
- Follows a series of other statutes, including:
  - The Provisions on Unreliable Entities;
  - The Rules on Counteracting Unjustified Extraterritorial Application of Foreign Legislation; and
  - The Anti-foreign Sanctions Law.

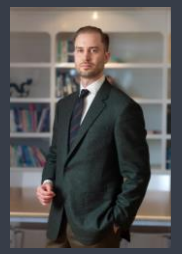
Counter-espionage Law (revised 2023)

- Key features
  - Broad definition of "*espionage*" – potentially including routine activities
    - "*illegally providing documents, data, materials, or other items related to national security and national interests*"
  - The terms "*national security*" and "*national interests*" are undefined
  - Requirement on closer collaboration between enterprises and state security organs
  - Increased risk for organizations and people who interact with foreign firms
    - Riskier for Chinese nationals to work for foreign firms in China
- Potential business impacts
  - Heightened risk for multinational companies who gather or have access to information
    - Foreign consulting and due diligence firms
    - Foreign law and audit firms
    - Client base
      - Defense industry
      - Financial and monetary
      - High-tech
      - Energy resources
      - Medicine and health and other key areas

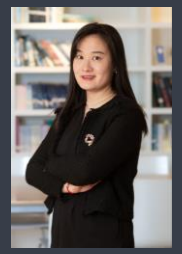
Law on Guarding State Secrets (revised 2024)

- Scope of restricted sensitive information expanded to include "*work secrets*" from 1 May 2024
  - Matters which are not state secrets but would cause a definite adverse impact after leaking
- Matters of science and technology may constitute state secrets
  - May restrict technology exportation
- Strengthens coordination with the data security law for management of confidential data
  - Electronic documents involving state secrets should be marked as state secrets

Thank you for your attention



Bård Breda Bjerken
Managing Associate
bbb@wrco.com.cn



Sherry Qiu
Senior Associate
shq@wrco.com.cn