Navigating China's Cybersecurity and Data Protection Policies

Sinolytics helps you successfully manage the impact of China's cybersecurity regulations on your business

Click here to contact us

sinolytics

Sinolytics: A European research-based consultancy focused on China

Profile

- Offices in **Berlin** and **Beijing**
- Nexus between **policy and business**
- Blending **in-depth research** with **management consulting** approach
- Bridgebuilders: **Diverse team** with European & Chinese perspectives
- Advising companies **across sectors** with focus on automotive, machinery, energy, chemicals, semiconductors
- **90+ clients**, including many of the largest and most respected foreign companies operating in China
- Founded in 2017

Key services

Regulatory Compliance	➢ Data-/Cybersecurity Regulation, Social Credit System, Environmental compliance
Geopolitical Advisory	➢ Geopolitics monitoring & forecasting, scenario building, impact assessment and mitigation
Supply Chain	➢ Definition of critical supplies, mapping tier-X supply chains, delivery failure assessment
Policy Monitoring	➢ Continuous, tailored policy and regulatory monitoring, trend detection and forecasting
Strategy Building	➢ Policy-driven strategy development, strategic positioning, and strategy implementation
Market Analysis	➢ Market intelligence for Automotive, Chemicals Semiconductors, Manufacturing, Machinery

Approach

Primary source and Chinese-language research

Problem-solving and developing tailored solutions

Dedication to deep research, cutting trough complexity

Depth in content, while strong in contextualization

Extensive expert network and research partners

sinolytics

1 **Sinolytics services: Cyber and data governance**

2 China’s cyber and data security regime: Trends, developments, enforcement

3 Regulatory deep-dive:
MLPS 2.0, cross-border data transfer, personal information, product compliance

China Cyber and Data Governance

Sinolytics' Service Scope

					Options for Sinolytics support
Module 1	Compliance risk assessment	Identify compliance risks/gaps	Action plan to compliance	Implementation of action plan	Conduct risk assessment, design action plan, support workstreams during action plan implementation, e.g. on cross border data transfer, PIP, MLPS 2.0 or product compliance
Module 2	Establish a PMO for HQ-local coordination	Steer HQ-local stakeholder coordination	Built-up internal structures that fit China-needs	Steer internal processes and progress control	Coordinate the process to identify stakeholders and assign responsibilities or take-over PMO role (for a transition period)
Module 3	Joint HQ-local strategy building	Mapping the risks (mid and long term)	IT set-up scenario building	Implementation plan	Analyze implication of IT set-up under different scenario and establish contingency plan
Module 4	Policy monitoring & adjustments	Cybersecurity monitoring and impact assessment	Re-visits of China IT strategy (on a needs basis)	Ad-hoc adjustments (on a needs basis)	Provide regulatory updates and alerts, support during strategy re-visits and adjustments if needed

Technical implementation partner

SigeniuS

Sinolytics Services

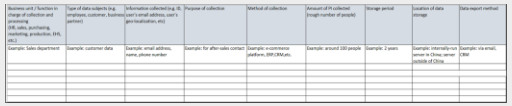
Deep-dive Module 1: Cyber and Data Security Risk Assessment

Risk Assessment

Four possible risk assessment areas, depending on your company's needs:
1 | Cross-Border Data Transfer (CBDT) – 2 | Personal Information Protection (PIP)
3 | MLPS 2.0 (network grading) – 4 | Product Compliance

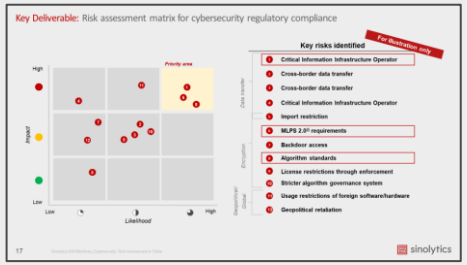
Baseline Analysis (Data/network mapping)

- Take stock of collected and stored data and/or product specifications and/or relevant operations, networks and services
- Identify key regulations and requirements with an impact on your company's cyber and data security and operations in China



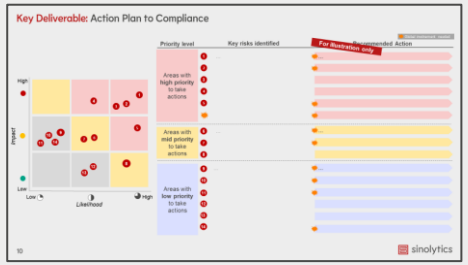
Self-Assessment & Risk Identification

- Identify and analyze risks to create initial risk matrix for your company's cyber and data security management related to China
- Risks are classified on a high-to-low spectrum with regards to their preliminary impact on the functions and compliance in China



Action Plan to Compliance

- Recommendations for action based on risk assessment
- Categorize recommendations by urgency and scope
- Design of an action plan to achieve compliance



Implementation

Implementation of Action Plan

- ✓ Compliance with China's **personal information protection** rules
- ✓ Compliance with China's **cross-border data transfer** rules
- ✓ Compliance with China's **network grading mechanism (MLPS 2.0)**
- ✓ **Compliance of your product(s)** with product-specific regulatory requirements
- ✓ Strengthen HQ-local cooperation
- ✓ Joint HQ-local strategy development & implementation

sinolytics

Sinolytics Services — Deep-dive Module 3: Re-thinking your China IT-strategy

- → Business and operational integration requirements to global & China IT systems can conflict with geopolitical & regulatory risks
- → Actual risk exposure and business/operation largely depend on local-global integration of business and current IT set-up
- → Detailed understanding of internal business needs and external risks is required to decide about scope and timing of IT separation

BUSINESS	OPERATIONS	REGULATORY	GEOPOLITICS
• China for global market • China for China • Global procurement from China • …	• Supply chain • Finance • R&D • Talent • …	• CBDT restrictions • Ban of foreign IT services • Accessibility issues (China Great Firewall) • …	• Sanctions • Different tech spheres • Network cut • …
Sinolytics value-add • Evaluate IT process needs from business • Assess how IT set-up can support China business	**Sinolytics value-add** • Evaluate the localization of applications based on operational needs	**Sinolytics value-add** • Identify compliance gaps/technical challenges • Set up mitigation plans	**Sinolytics value-add** • Analyze implication of IT set-up under different scenarios • Establish a contingency plan

Sinolytics experience: Chinese cyber regulations raise operational and strategic challenges

Case I: Cross-border transfer of cryptographic material

Proposition: Company A transfers cryptographic material (keys, certificates) from HQ in Germany to plants in China.

Key question: Is the transfer of cryptographic material to China allowed under newest cross-border data rules?

Challenge: Regulatory definitions of data requiring localization still in development.

Main choices: Leave current global infrastructure intact and risk non-compliance or localize infrastructure completely or partially in China at major financial cost.

Final decision: Full localization to pre-empt regulatory changes.

Case II: Choosing a cloud provider

Proposition: Company B is setting up a new cloud platform service in China.

Key question: Are Sino-US geopolitical tensions going to allow the use of US cloud providers in the future?

Challenge: Customers, especially SOEs, prefer usage of domestic alternatives.

Main choices: Incur costs by switching software to support Alibaba's cloud interface or use AWS and risk exclusion from the Chinese market in the long-term.

Final decision: Switch to Ali Cloud to increase level of local embeddedness .

Case III: Support for PIP compliance

Proposition: Company C is transferring customer and employee data through SAP to Germany

Key question: What are requirements to be compliant with cross-border data transfer of PI?

Challenge: Strict bureaucratic hurdles for companies to transfer data

Main choices: Continue using integrated ERP system or building up dual infrastructure system

Final decision: Strict implementation of requirements and continuation of globally integrated model

1 Sinolytics services: Cyber and data governance

2 China’s cyber and data security regime: Trends, developments, enforcement

3 Regulatory deep-dive:
MLPS 2.0, cross-border data transfer, personal information, product compliance

Cybersecurity is to strengthen China: National security, innovation, and privacy are key

The five main objectives of China's cybersecurity and data governance system

National security

China enhances cyber and data security measures as core aspects of national security

International cyber governance

China wants to be a cyber superpower and influence international rulemaking

Content control

China aims at absolute control of online content to ensure social and political stability

Consumer protection

China aims at addressing misuse of personal data, particularly in the digital sphere and the platform economy

Techno-nationalism

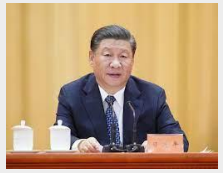
China aims at self-sufficiency by China-made technology

Digital economy

China wants to lead the world in digital economy and technologies

sinolytics

Its not just about regulations: Cyber and data security are on top-level national agenda



- Strong push towards **absolute control of the cyberspace** by Xi Jinping in July 2023
- Intensified, **campaign-style government action** with respect to cyber and data security to be expected

1 Xi Jinping stressed guiding principles of China's cybersecurity strategy

Party leadership

- Maintaining the Party's absolute control over cyberspace

China specific regulatory framework

- Maintaining China's own cyber management approach
- Strengthening the legislation, enforcement and judiciary

Security

- Building a strong national cyber security barrier 国家网络安全屏障

Ideology and social stability

- Strengthening positive energy 正能量 of internet content

Digital economy

- Promoting innovation in the cyberspace field
- Balancing both cybersecurity and internet development

2 Revision of Counter-Espionage Law poses further pressure to cross-boarder data transfer

The notion of espionage has been broadened to also include espionage activities related to data and cyber security

- *"Other documents, data, materials that compromise national security and interests"*
- *"Attack, invasion, disruption, control, damage on Critical Information Infrastructure"*

Allowing more investigation measures over company's data storage

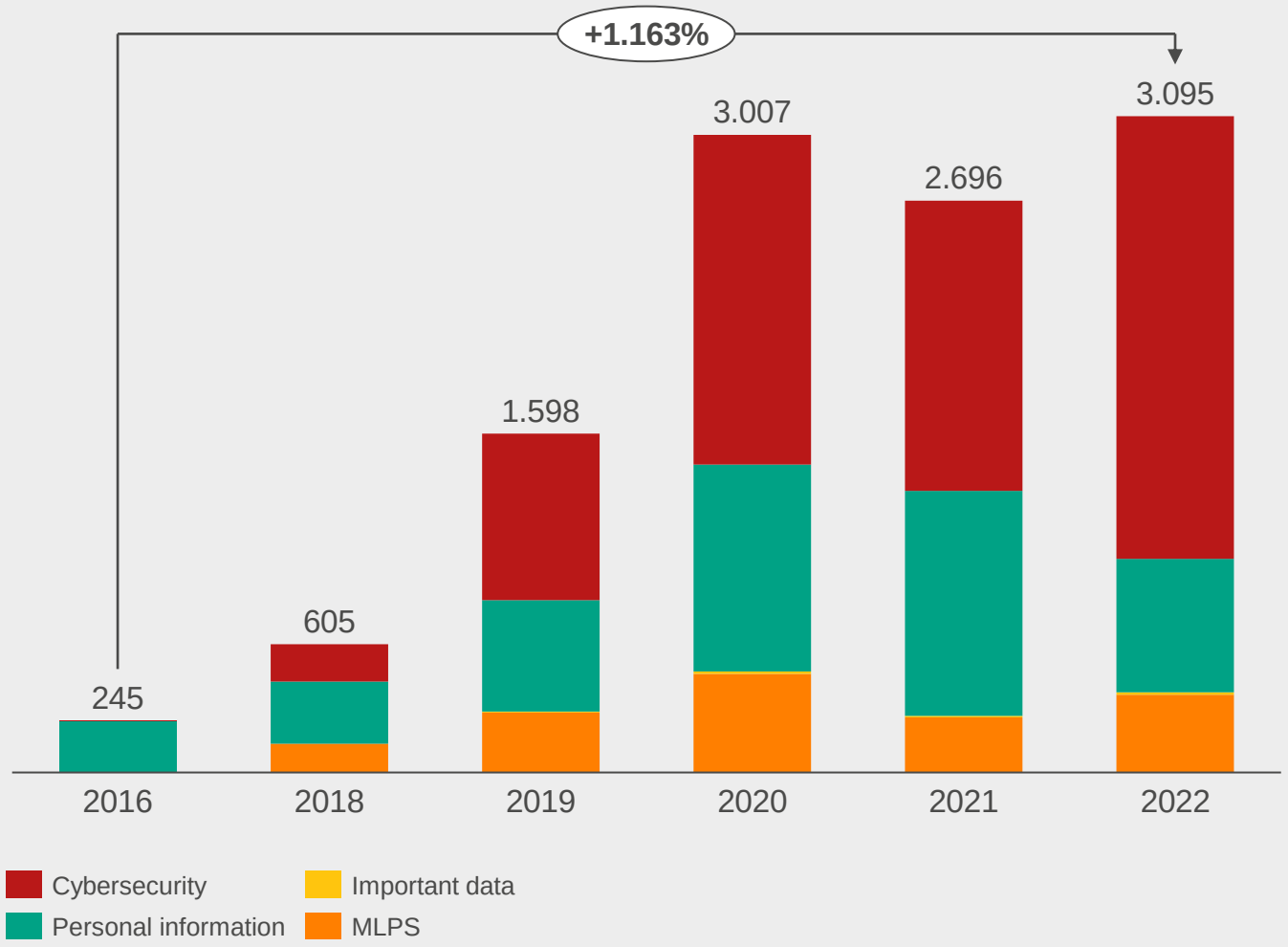
- *"Extracting and reviewing electronic data, summoning for investigation, and checking property information of suspects"*

Increased uncertainty

- If CN gov. tightens national security control, MNCs may face expanded scope of data deemed relevant to national security

Enforcement is picking up: Increase of cyber and data security-related fines

Number and reason of administrative fines for cyber/data security infringements



Source: Qichacha, as of 31 Dec 2022

Consequences of non-compliance

Depending on the severity
as judged by the Chinese regulator:

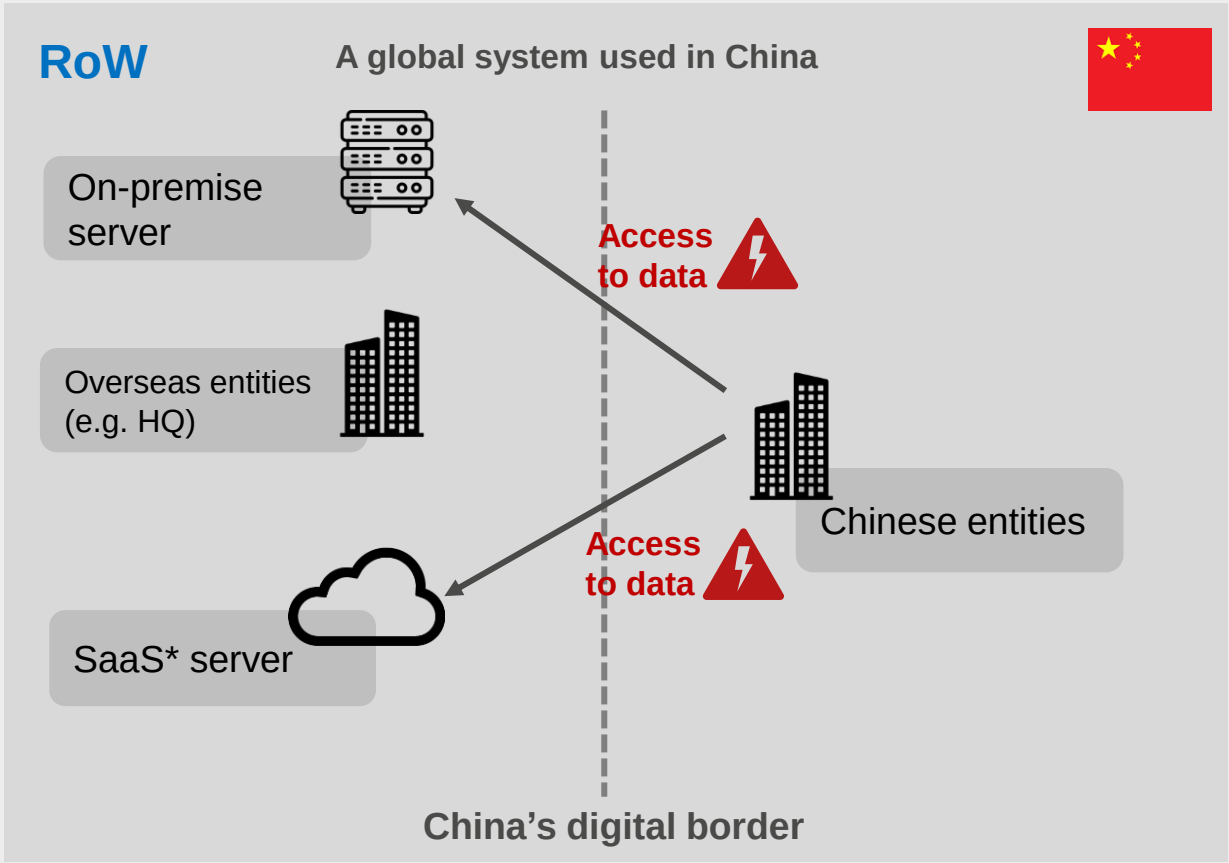
- Warning from the supervisors
- Fines from 50,000 RMB (6.7k EUR) up to 50 mn RMB (7 mn EUR) or 5% of last year's turnover;
- Fines for management: up to 1 mn RMB (140k EUR) per person
- Extreme cases: revocation of business license

→ **All fines are publicly visible in the entities' Social Credit Record and impact the frequency of government inspections.**

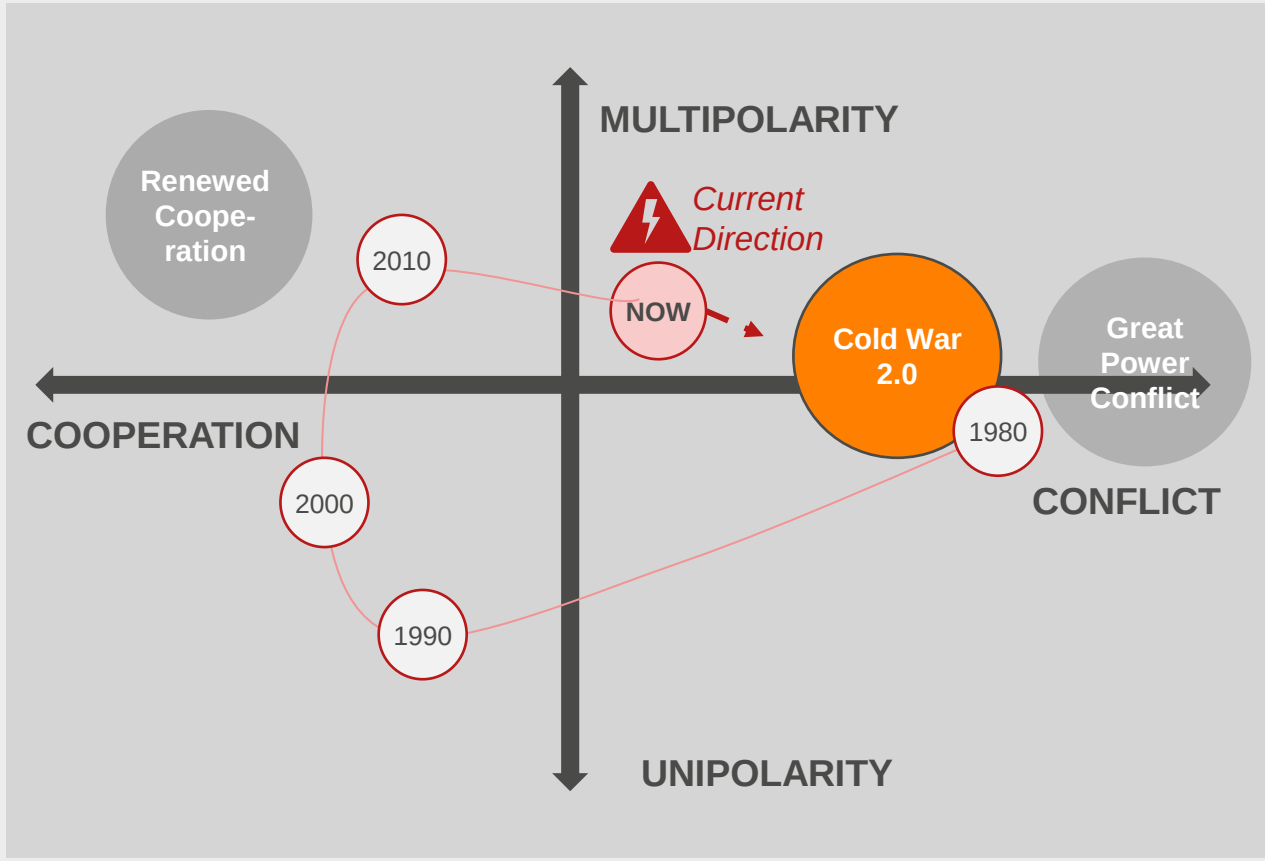
sinolytics

It won't get easier: Moving towards fragmented tech spheres and global IT separation

Cross-border data transfer is a matter of data sovereignty and national security…



…significantly impacted by the trend towards deglobalization and geopolitical tension.



sinolytics

Global tensions as an accelerator: It's time to start re-thinking your China IT-strategy

EXAMPLES – NOT COMPREHENSIVE

RISKS	RISK DRIVER	TREND
Accessibility issues	**Great Firewall** • Collaboration applications not working stably • Technical workarounds face disruptions	**Increase** Stronger regulation over unauthorized solutions
Security risks	**Ban foreign security services** • Security products face technical market entry barriers • Global solutions unable to deploy in China	**Increase** Full ban likely as geo-political tensions rise
Sales loss in CN	**IT localization requirements** • CIIO clients under pressure to screen suppliers • Suppliers forced to further localize	**Increase** CIIOs and suppliers held to rising compliance obligation
Sales loss in non-CN	**"China clean" product requirements** • China-free supply chain demands in sensitive sectors • Insurance against geopolitical sanctions	**Increase** Higher sensitivity for geo-political supply chain risks
Higher compliance cost	**Cross border data transfer restrictions** • Transfer of important data must be approved by CAC • Transfer of PI must go through SCC or certification	**Increase** Enforcement gaining momentum
Connection cut	**Geopolitical escalation** • WAN connection disrupted • CN business paralyzed if relying on global IT service	**Low** Low likelihood of escalation to this level in 5 years

IMPACT

Depends on

(a) Geopolitical development

(b) Corporate IT set-up

- Global process integration level
- Applications
- Infrastructure
- Security

1 Sinolytics services: Cyber and data governance

2 China’s cyber and data security regime: Trends, developments, enforcement

3 Regulatory deep-dive:
MLPS 2.0, cross-border data transfer, personal information, product compliance

Regulatory framework: Well advanced -- fine-tuning and stricter enforcement expected

Cyber- & Data Governance

Key laws	**Cybersecurity Law** (2017)	**Data Security Law** (2021)	**Data Privacy Law** (2021)

	1	2	3	4	5
Regulatory Tools	**MLPS[1] 2.0**	**Cross-border data transfer**	**Personal data protection**	**CIIO[3]**	**Network product and encryption**
	Grades networks based on degree of harm if system compromised	Outlines compliance procedures for classified important data[2] and sensitive personal data	Structurally similar to GDPR, requires to obtain user consent	Operators of key network facilities and systems in key industries i.e., finance, ICT, health etc.	Key products (incl. security) require a domestic sales license or security review
	→ *See slide 13-15*	→ *See slide 16-20*	→ *See slide 21-22*	→ *See slide 23-24*	→ *See slide 25-26*
Maturity	◕	◑	◕	◑	◑

Outlook

- Several rules still unclear, will be clarified, but leave room for ambiguity
- No significant new laws expected, rather re-visions, fine-tuning and focus on enforcement
- With US-China conflict escalating, willingness to politicize cybersecurity regulatory tools increases
  → see more on the impact of geopolitical tension on *slide 28-29*

1. MLPS: Multi-Level Protection Scheme
2. Important data: National and industrial specific guidance on important data identification is under drafting process.
3. CIIO: Critical Information Infrastructure Operator

1 MLPS 2.0 compliance: All firms operating networks must follow MLPS 2.0 requirements

MLPS 2.0 sets rules for all companies that operate networks (“network operators”) to increase **security protection capabilities**, including the ability to prevent threats, detect security incidents and recover after damage

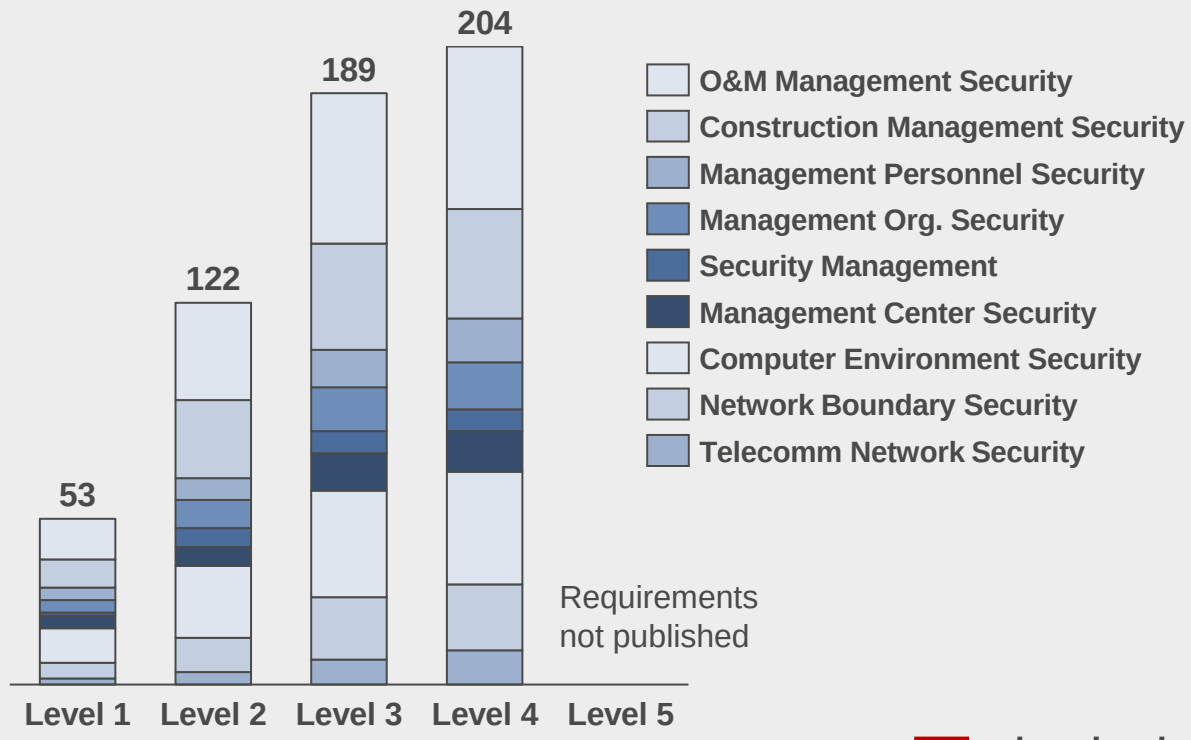
Companies need to grade their MLPS 2.0 level…

- Network operators are obligated to conduct a self-assessment
- Above level 2 are subject to extra expert evaluation
- Above level 2 need to file with local public security bureaus

	Level 1	Level 2	Level 3	Level 4	Level 5
Legal persons	Damage	Serious Damage OR	Very Serious Damage OR		
Public security		Damage	Serious Damage OR	Very Serious Damage OR	
Nat’l Security			Damage	Serious Damage	Very Serious Damage

…and comply with corresponding requirements

- The number of technical requirements in various security areas increase for higher MLPS 2.0 levels



sinolytics

Benchmarking: Examples of classifications from foreign and domestic companies

	Company	Industry	Network evaluated
MLPS 2.0 Level 2	BOSCH	• Manufacturing	• Corporate web portal
	Shanghai Yaohua Pilkington Glass	• Manufacturing	• Corporate web portal • Corporate ERP • Corporate office management system
	Feiliu Tech	• Infotech for the textile industry	• Smart manufacturing system for textile manufacturing
MLPS 2.0 Level 3	Shanghai Hongqiao Traditional Chinese Medicine Yinpian	• Pharmaceutical	• Intelligent management system for distribution of prescribed medication
	ABB	• Manufacturing	• ABB Ability™ (Industrial Internet of Things) • It not only collects health data from assets, but also involves automatic control and production implementation
MLPS 2.0 Level 4	Tencent Cloud	• Public cloud	• Tencent Finance Cloud
	Pingan Cloud	• Public cloud	• Pingan Cloud

Sinolytics Services

MLPS 2.0 (network grading) risk assessment

1 Baseline analysis

Level grading	• Network identification • Determination of MLPS 2.0 level • Support in compiling a self-assessment report for authorities
Requirement report	• List of requirements based on MLPS level

2 Compliance roadmap

Gap analysis	• Evaluation of current cybersecurity measures • Identification of potential compliance gaps with MLPS requirements
Implementation	• Roadmap with recommendations to close potential gaps • Identification of relevant documents and input for external review or filing • Identification of local accredited 3rd party reviewers for external review

3 Filing and certification

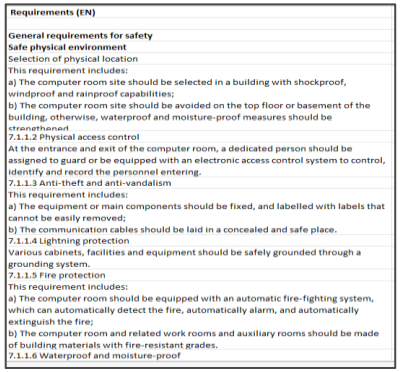
Process support	• Identifying suitable external agency • Guidance and review of MLPS 2.0 filing paperwork • On-the-ground liaison during MLPS 2.0 testing and filing

Technical implementation partner

SigeniuS

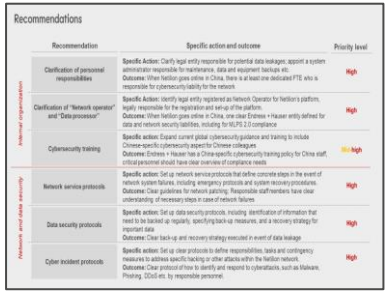
Sample deliverables

Requirement report


Requirements (EN)

General requirements for safety
Safe physical environment
Selection of physical location
This requirement includes:
a) The computer room site should be selected in a building with shockproof, windproof and rainproof capabilities;
b) The computer room site should be avoided on the top floor or basement of the building, otherwise, waterproof and moisture-proof measures should be strengthened.
7.1.1.2 Physical access control
At the entrance and exit of the computer room, a dedicated person should be assigned to guard or be equipped with an electronic access control system to control, identify and record the personnel entering.
7.1.1.3 Anti-theft and anti-vandalism
This requirement includes:
a) The equipment or main components should be fixed, and labelled with labels that cannot be easily removed;
b) The communication cables should be laid in a concealed and safe place.
7.1.1.4 Lightning protection
Various cabinets, facilities and equipment should be safely grounded through a grounding system.
7.1.1.5 Fire protection
This requirement includes:
a) The computer room should be equipped with an automatic fire-fighting system, which can automatically detect the fire, automatically alarm, and automatically extinguish the fire;
b) The computer room and related work rooms and auxiliary rooms should be made of building materials with fire-resistant grades.
7.1.1.6 Waterproof and moisture-proof

Action plan


Recommendations

Recommendation	Specific action and outcome	Priority level
Clarification of personnel responsibilities	Specific Action: Clarify legal entity responsible for potential data leakages; appoint a system administrator responsible for maintenance, data and equipment backups etc. Outcome: When Nellion goes online in China, there is at least one dedicated FTE who is responsible for cybersecurity liability for the network	High
Clarification of "Network operator" and "Data processor"	Specific Action: Identify legal entity registered as Network Operator for Nellion's platform, legally responsible for the registration and set-up of the platform. Outcome: When Nellion goes online in China, one clear Endress + Hauser entity defined for data and network security liabilities, including for MLPS 2.0 compliance	High
Cybersecurity training	Specific action: Expand current global cybersecurity guidance and training to include Chinese-specific cybersecurity aspect for Chinese colleagues Outcome: Endress + Hauser has a China-specific cybersecurity training policy for China staff; critical personnel should have clear overview of compliance needs	High
Network service protocols	Specific action: Set up network service protocols that define concrete steps in the event of network system failures, including emergency protocols and system recovery procedures. Outcome: Clear guidelines for network patching; Responsible staff members have clear understanding of necessary steps in case of network failures	High
Data security protocols	Specific action: Set up data security protocols, including identification of information that need to be backed up regularly, specifying back-up measures, and a recovery strategy for important data Outcome: Clear back-up and recovery strategy executed in event of data leakage	High
Cyber incident protocols	Specific action: Set up clear protocols to define responsibilities, tasks and contingency measures to address specific hacking or other attacks within the Nellion network. Outcome: Clear protocol of how to identify and respond to cyberattacks, such as Malware, Phishing, DDoS etc. by responsible personnel.	High

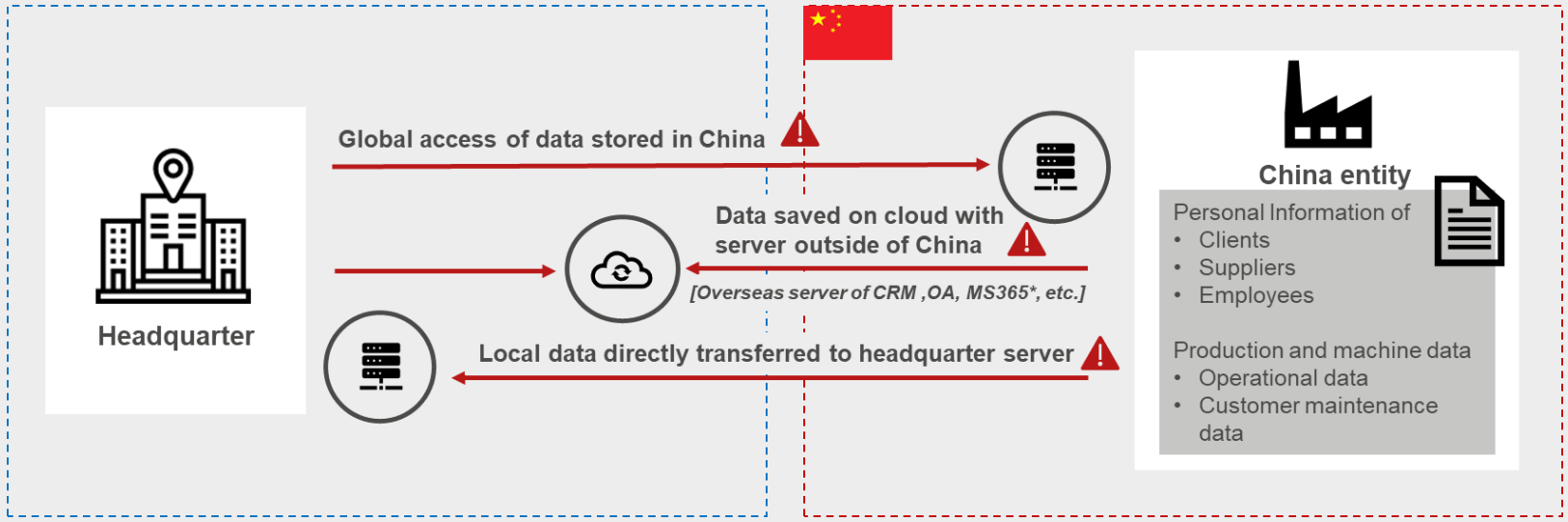
Documents for MLPS filing

sinolytics

2

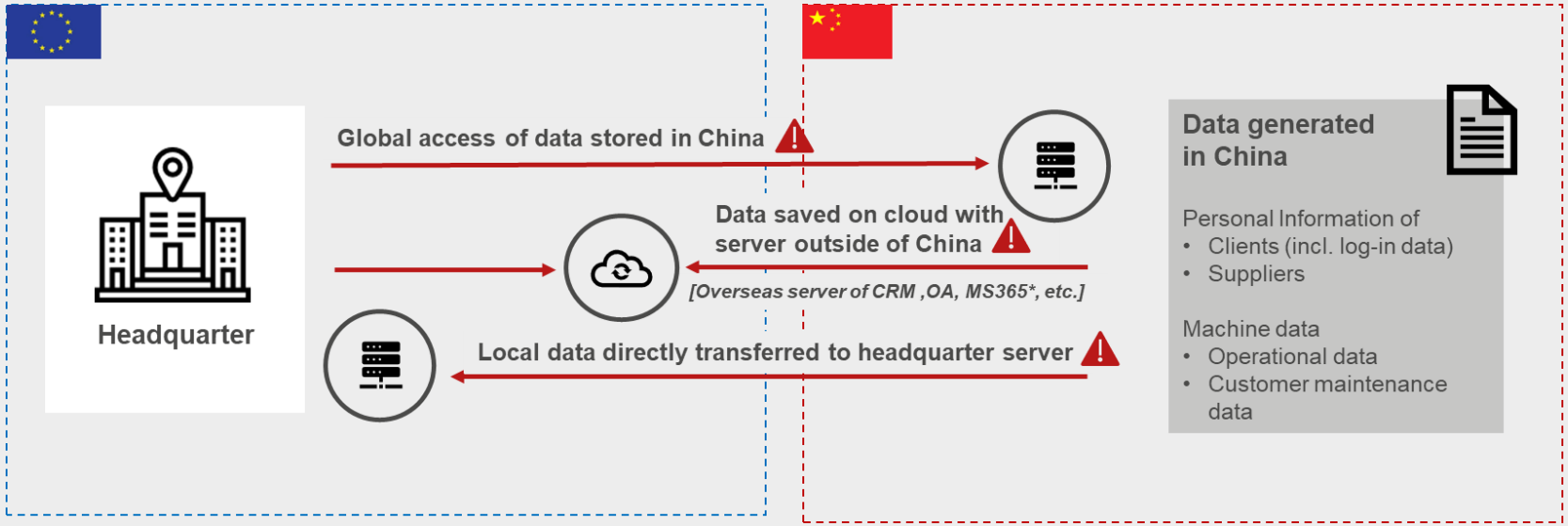
Cross border data transfer scenarios: Increased compliance risk in global data flows

→ Scenario 1: Entity in China (with key functions like production, sales, and R&D)



Cross-border data transfer risk alert

→ Scenario 2: No entity in China (only sales to China)



sinolytics

2

Compliance options: Decision tree for cross border data transfer assessment

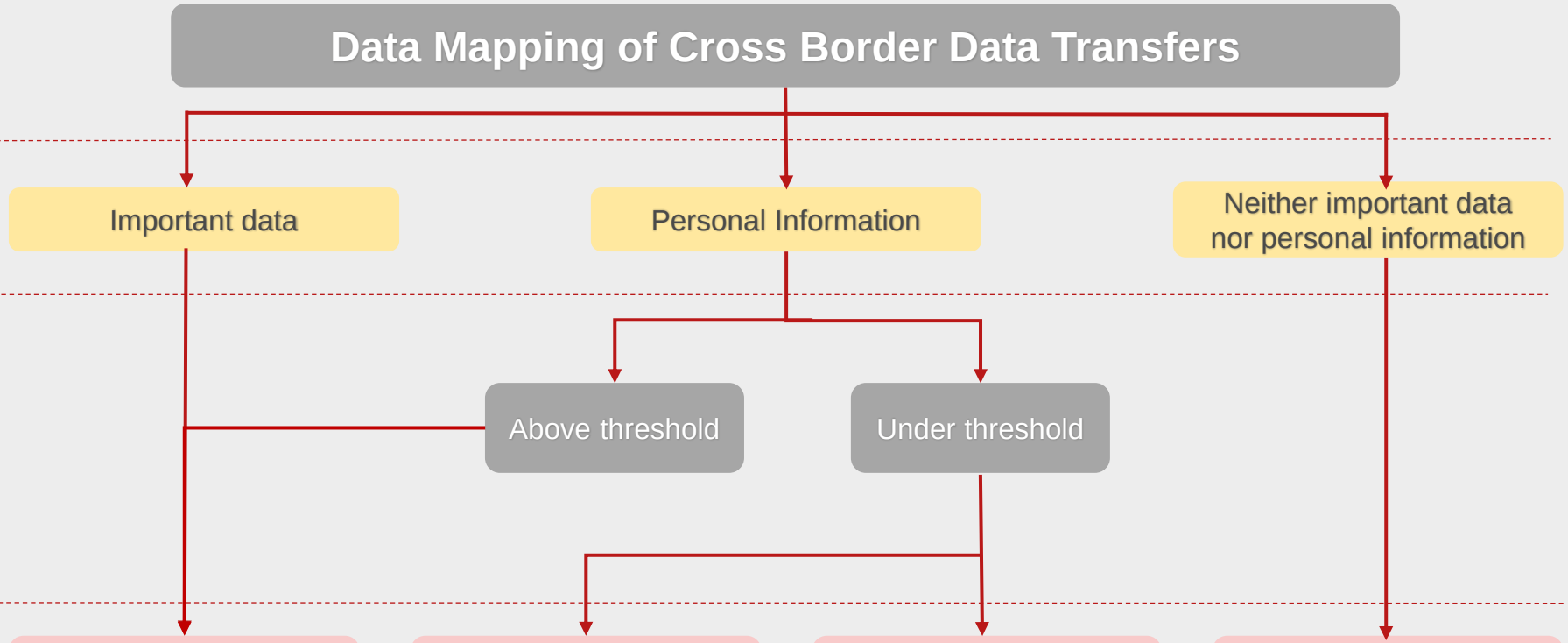
Data mapping: Analyze data by purpose, size, scope, type and sensitivity

Data classification: Identify important data and personal information → *see next slide* !

Data volume: Assess the personal information threshold

PI of 100,000 people (cumulative since Jan. 1 the year before); sensitive PI of 10,000 people (cumulative since Jan. 1 the year before); PI threshold doesn't apply to CIIOs and entities managing PI of >1 million people. Any PI transfer by them requires security assessment

Compliance: Choose the right CBDT mechanisms



- Lengthy process
- High costs
- Heavy paperwork
- Dealing w/ regulator
- Long waiting time

- PI transfer between subsidiaries of MNC
- Similar to Binding Corporate Rules

- Simple but w/ strict requirements
- No 3rd Party involved
- Similar to GDPR
- Official template

! CIIO[3] clients may request their data to be stored in China to fulfill CIIO-specific regulations

Data localization can reduce compliance costs and risks

1| CAC: Cyber Administration of China
2| PIP: Personal Information Protection
3| CIIO: Critical Information Infrastructure Operator

sinolytics

2 Data classification: Methods to narrow down the scope of potentially important data

1 Identifying data to be graded → 2 Identifying objects to be impacted → 3 Assessing level of impact

Key factors to define scope of important data:

- Data reflecting national strategic reserves and emergency mobilization capacity
- ▲ , genetic information, etc. Data supporting CII operations or industrial production in core sectors
- Data reflecting CII security protection
- ▲ Data related to export control items
- Data that could be used to initiate a military attack against China
- Data reflecting location of key targets, important sites or undisclosed geographical targets
- Data that could be used to launch network attacks to destroy the supply chain of key equipment and system components
- Data reflecting health and physiological status of the population, ethnic characteristics
- Data related to natural resources and the environment
- Data related to scientific and technological ▲ advancement and the country's competitiveness
- Data related to the production and trading of sensitive items and equipment
- Data generated in the course of providing ▲ services to government agencies, military enterprises and other sensitive and important institutions

	Limited impact	Average impact	Severe impact
National security *(politics, land, military, economy, culture, society, technology, electromagnetics, network, ecology, resources, nuclear safety, overseas interests, biology, space, polar regions, deep sea, artificial intelligence, etc.)*	Important data	Core data	Core data
Public interest *(society, industries, regions, etc.)*	General data	Important data	Core data
Rights and interest of ***individuals and organizations***	General data	General data	Important data

▲ Items potentially impacting international companies

Source:
Management measures for data security in industry and information sectors, MIIT, 2022;
Guidelines for identification of important data (draft), 2022, SAMR

2 Standard Contract: Contracting between data processor and overseas recipient

Scenarios of Standard Contract:

- Non-CIIOs
- Entities managing PI of <1 million people
- PI of < 100,000 people (cumulative since Jan. 1 the year before)
- Sensitive PI of <10,000 people (cumulative since Jan. 1 the year before)

Implemented since 1st June 2023 with a transition period of 6 months

PIP Impact Assessment

- Legality, legitimacy and necessity
- Size, scope, type and sensitivity of data
- Risks to individual rights and interests
- Recipient obligations and security capabilities
- Risk of data being compromised after transfer
- Channels for addressing user rights
- Impact of recipient country/region's PIP laws and regulations on performance of contract

Standard Contract

- Basic info of PI (personal information) handler
- Info of related business and system
- PI to be transferred
- PIP capability of PI handler
- Information on overseas recipient
- Information on overseas recipient
- Cross-border data transfer impact assessment

Other supporting documents

- Photocopy of social credit code certificate
- Photocopy of legal representative's ID card
- Photocopy of the identity card of the person in charge of the filing process
- Power of Attorney
- Commitment letter

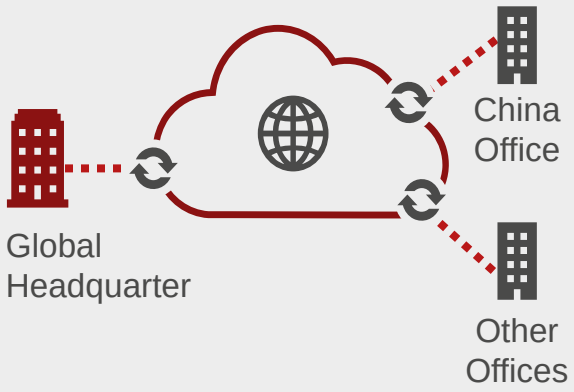
Submit all required materials

Filing with authority

- Company should file with provincial CAC within **10 working days** after the contract goes into force
- CAC should review materials within **15 days**
- If any revision needed, company should submit the updated materials within **10 days**
- CAC will provide company a **filling number** after approving the filing of standard contract

Company should follow the templates provided by CAC

Cross-border data transfer (CBDT) risk assessment



1 Data mapping: Sinolytics analyzes your CBDT risk levels

- Goal: **Identify sensitive & important data flows** that require localization & higher compliance, today/future
- **Data mapping**: Sinolytics conducts data mapping, classifying each data flow by data storage, volume and sensitivity and mapping data flows by their risk levels, considering existing and potential future regulatory requirements
- **Risk matrix:** Based on likelihood and impact

2 CBDT verification: Joint identification your risk acceptance level

- Goal: Based on your company's China business strategy, evaluate which **level and type of cross-border data transfer is necessary and which data/application can be localized**
- **Business needs**: Sinolytics conducts systematic interviews with commercial functions/ R&D to assess which data/applications can be localized, which data can be anonymized, which adjustment of business/innovation process are feasible etc.

3 IT scenario: Specification of IT adjustment options

- **Benchmarking**: Sinolytics provides insights from best practices and benchmarking case studies to derive an optimal IT setup
- **Strategic IT options**: The IT solution options consider **adjustments to infrastructure (cloud, networks) and applications at global and local level.**
- **Cost and benefit analysis**: Weighing the benefits of risk mitigation against the costs of IT adjustments
- **Resource allocation**: Assess timeline and costs of implementation; define workstream involvement

3 Personal data protection: Wide-sweeping impact on different departments

- China's 2021 Personal Information Protection Law (PIPL) sets out framework requirements for companies to protect personal information they collect and process

Business Function	(Sensitive) Personal Information	Impact on operations
Human resources	• Employees' address, personal phone number, e-mail address • Position, work unit, education, degree, education experience, work experience, training record, transcripts	• PIPL allows only limited personal information collection without individual consent (for some HR functions)
Finance and accounting	• Bank account, deposit information (including the amount of funds, payment collection records) • Client's name, address, personal phone number, photos, nationality, job position	• Financial personal information face specific categorization • Certain categories of sensitive financial personal information may need to be localized
Marketing/ e-commerce	• Clients' address, personal phone number, e-mail address • Software usage records, click records, favorite lists • Transaction and consumption records	• Personal pricing algorithms and automated decision-making through big data analysis are completely prohibited by the new PIPL and supporting regulations

Source:
Personal Information Protection Law, 2021
GB/T 35273 Personal Information Security Specification, 2020

Implications for Companies

- Individual (retractable) consent required for all PI collection
- Companies should segment sensitive personal information processing and develop separate consent mechanisms
- For cross-border personal information transfer, companies need to conduct impact assessments and sign contracts with foreign data recipients
- For cross-border data transfer, companies need to demonstrate that data transfer abroad is necessary
- Penalties for non-compliance can reach up to 50 mn CNY or 5% of annual revenue

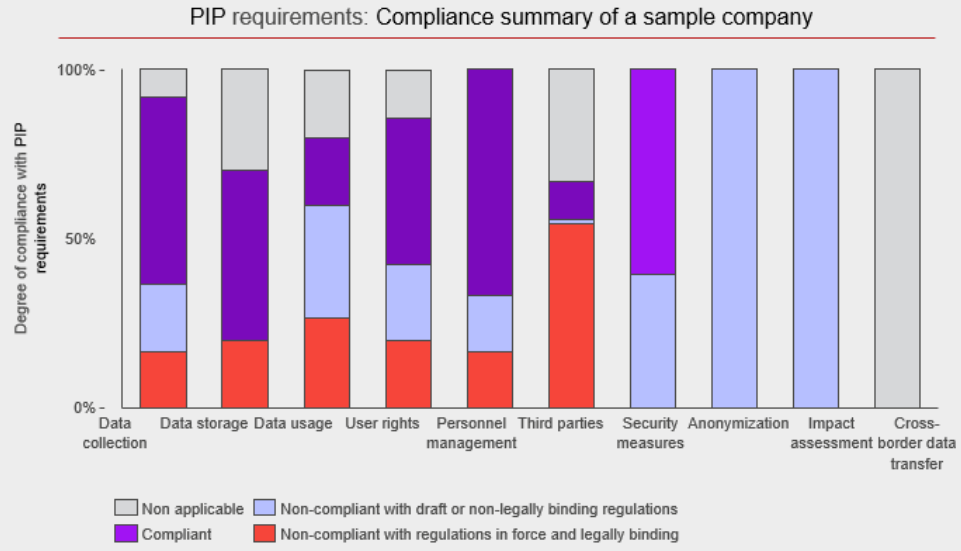
Personal information protection risk assessment

Sinolytics examines company compliance with 500+ requirements for personal information protection

Regulatory Areas covered by our compliance analysis:

- Data Collection
- Third Party
- Data Storage
- Security Measures
- Data Usage
- Anonymization
- User Rights
- Impact Assessment
- Personnel Management
- Cross-border Data Transfer

Case-study: personal information protection (PIP) requirement analysis



Main action areas for companies

- **Reviewing** consent notifications
- **Creating mechanisms for** PI subjects to access, correct and delete their PI
- **Ensuring internal process for PI personnel and management**
- **Third parties: Revising contracts to e**nsure third party PIP compliance
- **Impact assessment:** Analysis of risks and protective measures for a range of PI processing activities

sinolytics

sinolytics

4

CIIO & suppliers to CIIOs: Likely to hold important data, with major consequences

- Foreign company can face increasing pressure from potential CIIO clients who are required to screen suppliers to ensure supply chain security.

CIIOs are likely to be in critical industries…

CIIOs are companies that may "***gravely harm national security, the national economy, the people's livelihood and the public interest if sabotaged***"

Finance	• Bank operators • Securities and futures trading • Insurance
Telecomm.	• Data center/cloud services • Voice, data, internet network and hubs
Health	• Health institutions such as hospitals • Disease control • Emergency centers
Manufacturing	• Intelligent manufacturing system • High-risk industrial facilities
Water conservancy	• Long-distance water delivery • Urban water source
Energy and chemical	• Oil and gas extraction • Refining and processing • Oil and gas storage
Known CIIOs	DiDi, Sinopec, WeChat, 支付宝 ALIPAY

…which map onto important data areas

- **Economic operations**
  e.g.: strategic reserve data (e.g., food)
- **Population and health**
  e.g.: unpublished health stats
- **Science and technology**
  e.g.: major national S&T plans and planning data
- **Security protection**
  e.g.: data from key national production sites
- **Government affairs**
  e.g.: non-secret government data
- **Application services**
  e.g.: automotive data collected across country
- **Natural resources and environment**
  e.g.: mapping and geological data

CIIOs face stricter requirements…

Asset risk assessment: CIIOs must conduct a **risk assessment of all assets**

Data storage: CIIOs must store important and sensitive personal information in **separate data servers within China**

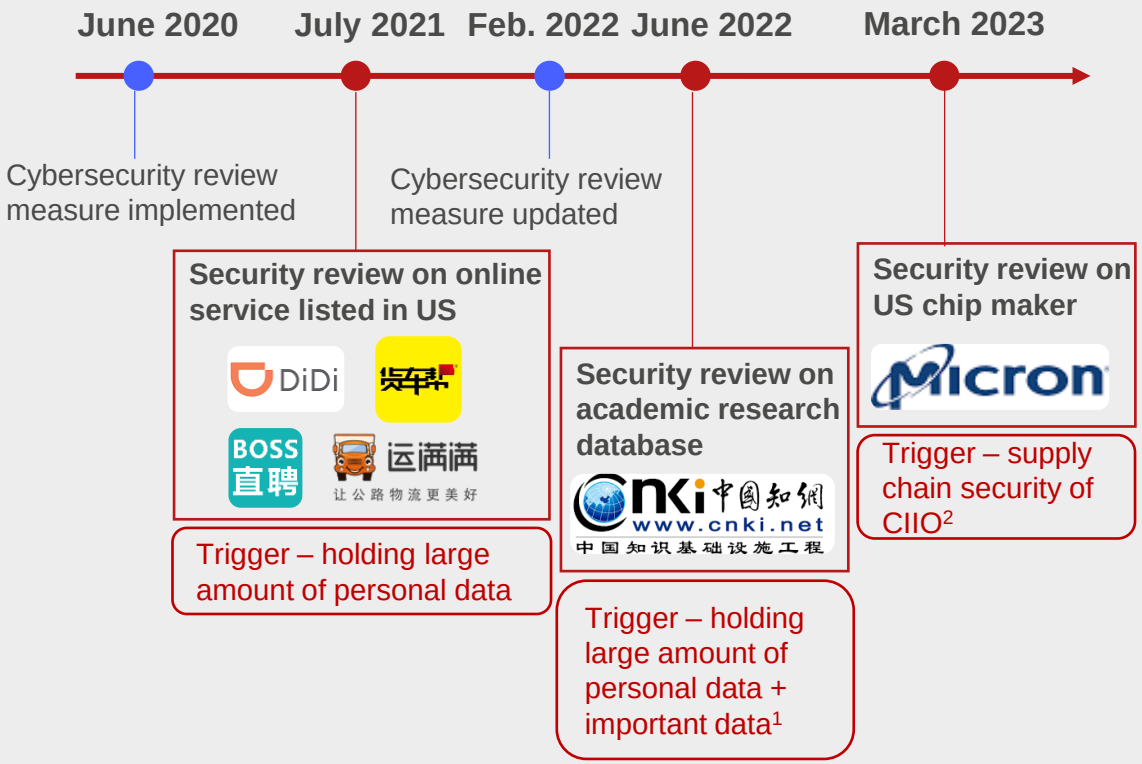
Post-incident recovery: Post-cyber incident recovery requires **instant back-up system**

… as well as suppliers to CIIOs

Supply chain: **Network and service providers** to CIIOs must undergo cybersecurity review procurement procedures

Data localization: suppliers face pressure from CIIO clients to localize client-related data

Case study: Micron has been banned from supplying to CIIO due to security concerns



1 Important data:data with a national security, national economic, social stability, public health and safety or other public interest dimension
2 CIIO: critical information infrastructure operator
Source: Cyberspace Administration of China (CAC)

Micron case – first cybersecurity review of a foreign company

- **Focus on supply chain risks:** On 31st March 2023, the Cybersecurity Review Office under the Cyberspace Administration of China (CAC) launched a cybersecurity investigation into the local sales of US memory chip company Micron. Official reason was concerns about supply chain security of critical information infrastructure (CII).
- **Political motivations to retaliate against US restrictions:** China's probe into Micron followed sweeping restrictions introduced by the US on China's semiconductor industry in October last year.
- **Micron was highly responsive to the US call to reduce China exposure**: Reduced the number of Chinese staff and closed operations at its Shanghai chip design center in January 2022
- **Micron was banned from supplying CIIOs:** On 21st May 2023, CAC announced that Micron's products pose significant security risks to China's CII supply chain and Micron products will be banned from CII. In theory, Micron can still supply to non-CIIO clients in China.

Implications for your business

- Identify existing or potential CIIO clients among your client base in China
- Assess the significance/sensitivity of your products or services supplied within the CIIO's supply chain
- Closely monitor the sales requests from CIIO clients, especially for data system localization/separation

Network product compliance: Pre-sales certification is needed for selected products

- "*Critical network product and dedicated cybersecurity products* shall comply with the **mandatory requirements** of relevant national standards and are required to either obtain **security certification** from accredited certification bodies or pass **security inspection** before they can be put on sale or supplied in China." --- Article 23 of the China Cybersecurity Law

Regulatory evolvement: Mandatory standard published in 2021

June 2017
- The first catalogue of critical network products published 网络关键设备和网络安全专用产品目录（第一批）

June 2018
- CAC, MIIT, PBS and CAA* published a list of qualified certification and inspection institutes 安全认证和安全检测任务机构名录（第一批）


国家互联网信息办公室
中华人民共和国工业和信息化部
中华人民共和国公安部
中国国家认证认可监督管理委员会
公　告
2017 年　第 1 号
关于发布《网络关键设备和网络安全专用产品目录（第一批）》的公告

Feb. 2021
- Mandatory standard: General Security Requirement for Critical Network Products (GB 40050-2021) 网络关键设备安全技术通用标准


GB
中华人民共和国国家标准
网络关键设备安全技术要求
通用要求

Feb. 2022
- Siemens, as the first company obtained inspection report for their PLC product

Oct. 2022
- CICS-CERT* organized the set-up of specific security inspection standards for critical network products of PLC

July 2023
- Announcement on the Adjustment of the Catalogue of Network Products and Special Products for Network Security

If failing to fulfill mandatory req., company will face sales ban

If a company sells critical network products in China without meeting the mandatory standards and passing certification/testing, it will face the following negative impacts

Type	Impact	Seriousness	Likelihood
Warning	Company will be forced to pass certification/testing	Low	Mid
Sales ban	If company cannot pass the testing, company cannot sell relevant products	High	Low
Sales loss	CIIO* clients choose not to purchase uncertified products	High	High

*CIIO: critical information infrastructure operator

5

Encryption import license: A chokepoint for selected foreign companies

- New Encryption Law relaxes rules for foreign encryption products, but **products covered by import list still need to apply for a license** to enter the Chinese market

In 2019, NPC approved China's Encryption Law


中华人民共和国密码法

（2019年10月26日第十三届全国人民代表大会常务委员会第十四次会议通过 ）

Article 25 — **Voluntary mechanism**
Law encourages, but not mandates, enterprises to voluntarily apply to qualified testing and certification

Article 26 — **Mandatory mechanism**
If national security, welfare or public interest is concerned certification can be mandatory

Article 27 — **Critical Information Infrastructure**
Critical Information Infrastructure Operators have to carry out commercial encryption security assessments

Article 28 — **Licenses**
OSCCA and MOFCOM are tasked with testing and export/import licensing that involve national security

2020 introduction of encryption import / export list

- The Encryption Import / Export List serves as specification to Article 28 of the Encryption Law

Products covered by import list

- Commercial passwords used in mass consumer products are not subject to import licenses
- Only includes four types of commercial encryption hardware:
  - Encrypted phones
  - Encrypted fax machines
  - Crypto machines (including crypto cards)
  - Encryption VPN hardware devices

Licensing procedure

- Importers must submit an application with MOFCOM for the *Encryption products and equipment containing encryption technology import license*（密码产品和含有密码技术设备进口许可证)
- Importer needs to provide details, such as
  - Technical description of commercial ciphers
  - End user and end use certificate

sinolytics

Your contact at Sinolytics:

Mirjam Meissner | Managing Partner
Email to: mirjam.meissner@sinolytics.de