Cybersecurity Law and Data Protection Compliance for the China Market 2019

Survey & Report

BUSINESS
IS
GREAT
BRITAIN & NORTHERN IRELAND

Foreword

With the rapid evolution of the information technology environment, businesses and governments around the world are confronting digital risk. Security threats such as network attacks, network intrusions and malware are growing in sophistication. On the other hand, widespread privacy concerns emphasise the importance of personal data protection. As governments develop national regulatory frameworks to cope with these new challenges, companies are adapting their data management systems across multiple jurisdictions.

Against this backdrop, China adopted its first comprehensive legislation governing the area in the Cybersecurity Law of the People's Republic of China in 2017. The law affects organisations that deal with consumers and businesses in mainland China and will transform the way that data is collected, stored, used, disclosed and disposed of.

Although the precise applications of some provisions of the Cybersecurity Law are still subject to further clarification, it has drawn significant attention from the business community. Some enterprises are looking to best practice to set up internal safety management systems for data protection; others are concerned with the restrictions imposed on companies' China operations that have been ushered in by the new law.

In order to better understand the British business community's reaction to China's cybersecurity regime, the UK's Department for International Trade (DIT), LexisNexis, Zhong Lun Law Firm and the China-Britain Business Council (CBBC), carried out a survey in the first half of 2019. Nearly 80 British companies provided responses to an online survey, while leading cybersecurity experts were interviewed face to face.

The data collected from the survey was used to identify and assess, from the perspective of British business, 1) the key challenges; 2) current understanding of the law's key components; and 3) the measures taken in response. It is hoped that this will identify the law's key areas of impact and concern to UK business.

With these perspectives in mind, the survey is followed by an overview of China's cybersecurity regime, exploring the following key areas:

- Overview of the regulatory framework;
- Key compliance recommendations for British companies;
- Best practice of Chinese companies.

Put together, the survey and subsequent analysis aims to take stock of the Cybersecurity Law's impact on British business. It is hoped that this information will also help the British business community to greater understand its key provisions, manage risks and ensure compliance.

Michael C Jones

RELX Group Chief Privacy Officer

Table of Contents

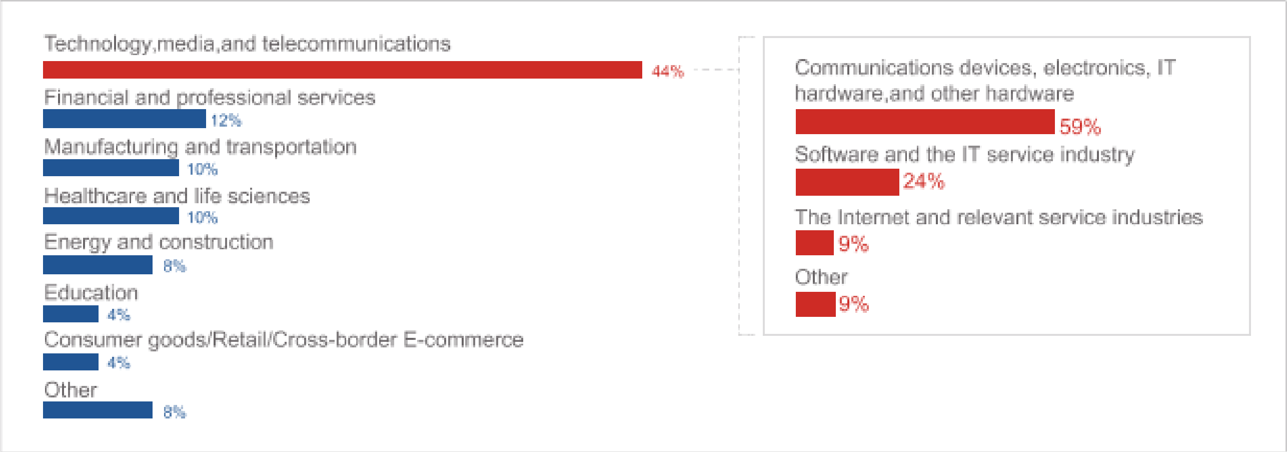
Part I Survey Result Analysis

The *"Market Access Survey - Cybersecurity Law and Data Protection Compliance for the Chinese Market"* took the form of an online questionnaire consisting of multiple-choice questions. The survey was launched on March 12th 2019 and was publicly available until May 31st 2019. Numerous channels were used to reach out to over 800 UK companies, receiving a total of 78 responses from British companies of various sizes and industries operating across China.

Executive summary

1.1 Profile of the Respondents

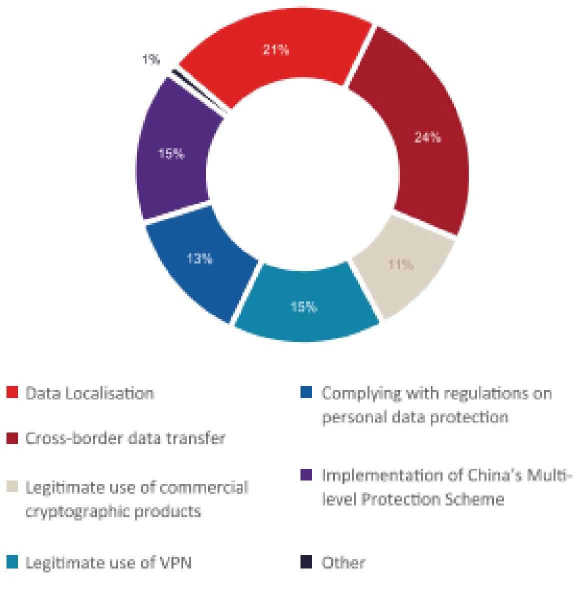
The survey gathered the views of a large cross-section of British business. Nearly half (44%) of the respondents were members of the C-suite (CEO, CIO, Chairman, CTO, etc.). Our interviewees covered both small- and medium-sized enterprises (SMEs) and multi-national corporations (MNCs). The majority (76%) of the respondents were already established in the China market, whilst 24% of them were exploring the possibility. Just under half (45%) of the respondents were from the ICT (Information and Communication Technology) sector.



1.2 Major Challenges

With respect to the major challenges for UK Business, the top four major challenges are data localisation (21%), cross-border data transfer (24%), implementation of China's multi-level protection scheme (15%) and legitimate use of VPN (15%). Moreover, we cross-analyse the data against the factor of whether a business has already entered the China market, and according to our result, UK companies which operate in China consider data localisation to be the biggest challenge, while UK companies which sell to Chinese customers from overseas and/or sell via local partners believe that cross-border data transfer is the major challenge .

Which of the following requirements do you consider to be major challenges for your company's China operations?



1.3 Data Collection and Cross-border Transfer

As the Cybersecurity law centers on the governance of data, the survey probed industry perspectives on some of its key requirements. The collection of personal information and important data requires compliance with security measures, while data collection and cross-border data transfer are subject to security reviews.

- Regarding the collection of **Personal Information**, 45% of UK companies operating in China collect Personal Information directly or indirectly, while 50% of those considering entering the China market believe they would engage in the collection of Personal Information. This demonstrates the pervasiveness of data collection as a business activity, and the extent of the CSL's application.
- Regarding **Important Data**, the survey revealed that a larger percentage of companies were unsure of the scope of its application, reflecting uncertainties with its current legal definition .
- On the issue of **cross-border data transfer**, 41% of the respondents with China-incorporated operations believe that it will be a game-changer if they are unable to access or collect data in China in a compliant manner, while 35% of the respondents believe that it will be a game-changer if they are unable to transfer data cross-border in a compliant manner. The survey also revealed that multinationals were more concerned about cross-border data transfer, while SMEs were focused primarily on data access and collection.
- In regard to **Critical Information Infrastructure Operators (CIIOs**[1]**)**, of those respondents who have already set up operations in China, only 33% have assessed the possibility of itself or its customers being designated as a CIIO . As CIIO designation entails greater compliance burdens and scrutiny, this suggests the need for greater awareness.

1.4 Reactions from the British Business Community

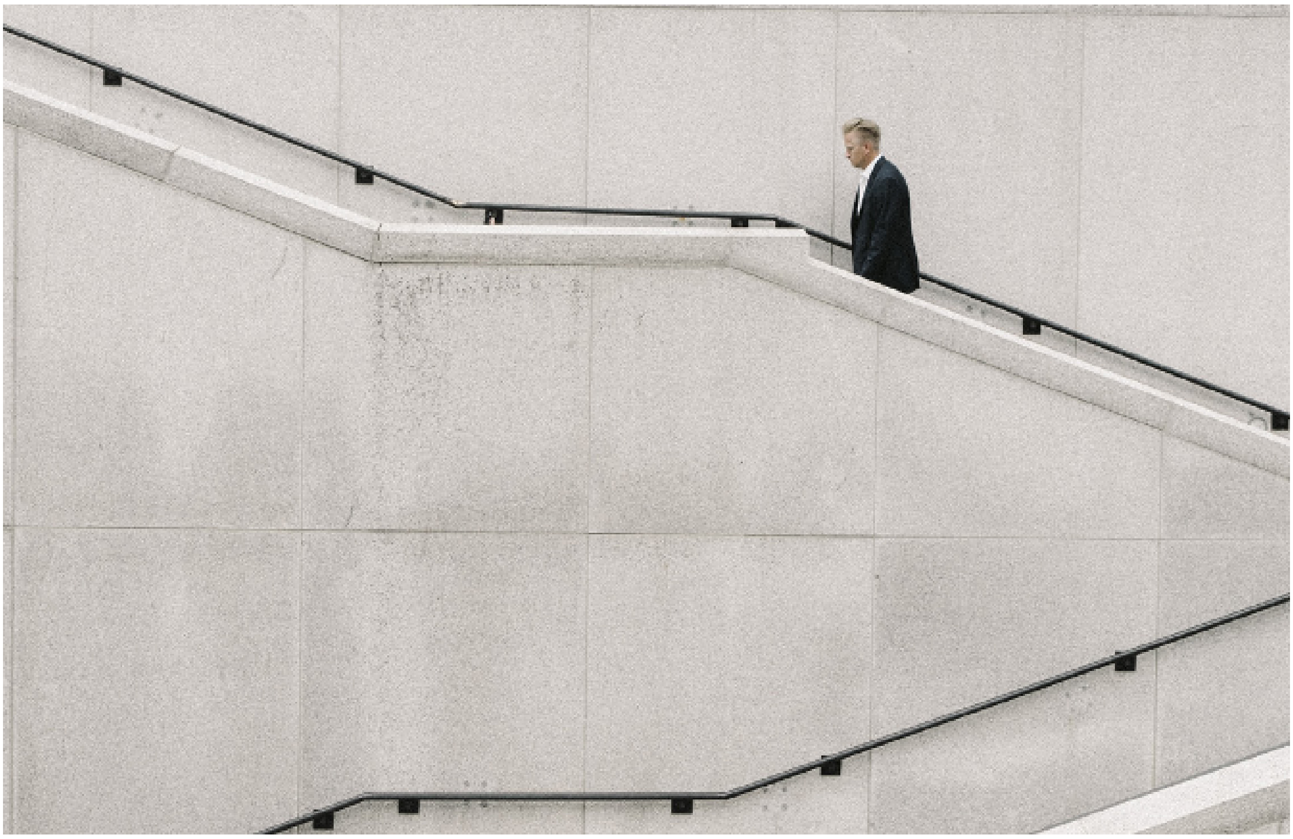
- In regard to the **compliance measures** that UK companies have undertaken thus far in response to the cybersecurity law, the survey indicates that companies remain in early stages. While 48% of the respondents have appointed a specific person to oversee cybersecurity and data compliance work for its China operations, only 27% of the respondents have set up internal safety management systems and

[1] Critical information infrastructure refers to information facilities that directly concern national security and stability and may seriously endanger national security and public interest. While further implementing regulations are expected, the sectors that have been explicitly named include energy, finance, transportation, education, scientific research, water conservancy, industrial manufacturing, healthcare, social security and public utilities

operating procedures. Furthermore, less than half have adjusted, or considered adjusting, their IT architecture in China to the requirements of data localisation. While this may indicate lack of preparation on the side of UK companies, it also reflects that many of the measures remain in draft form.

- In regard to professional advice, the top three external parties that UK companies consulted regarding cybersecurity issues are the Department for International Trade (DIT) (22%), professional service providers (22%) and the British Chamber of Commerce in China (BCCC)(13%). It shows that a large number of enterprises have begun to take stock of data compliance obligations. However, responses indicate that compliance efforts are mixed and companies have yet to implement a robust compliance mechanism.
- Regarding the **impact on business operations** of the Cybersecurity Law, 76% of the respondents believe that China's current legislation and policies on cybersecurity will affect operations in China; 16% of the respondents believe that it will restrict product innovation, 12% of the respondents think that it will cause delays in accessing the China market and 22% of the respondents believe that it will restrict marketing activities. Despite the challenges and restrictions, 49% of the respondents believe that the Cybersecurity Law and its implementation will promote a healthier business environment and help to protect personal privacy .
- **Recommendations** - 71% of the respondents believe that bilateral or multilateral data flow mechanisms between countries will benefit UK enterprises. Up to 74% of the respondents called for **greater exchange and communication** between companies and government agencies from the UK and China.

Overall, the survey has provided a useful overview of the British Business Community's views and reactions to the Cybersecurity Law in China, as well as revealing the key areas of impact and concern. Although the law's implementing measures are still under review, this information will help the DIT to provide targeted case-by-case support to companies, and secure a more optimal business environment for British business in China.



Part Ⅱ

Overview of China’s Cybersecurity Regulatory System

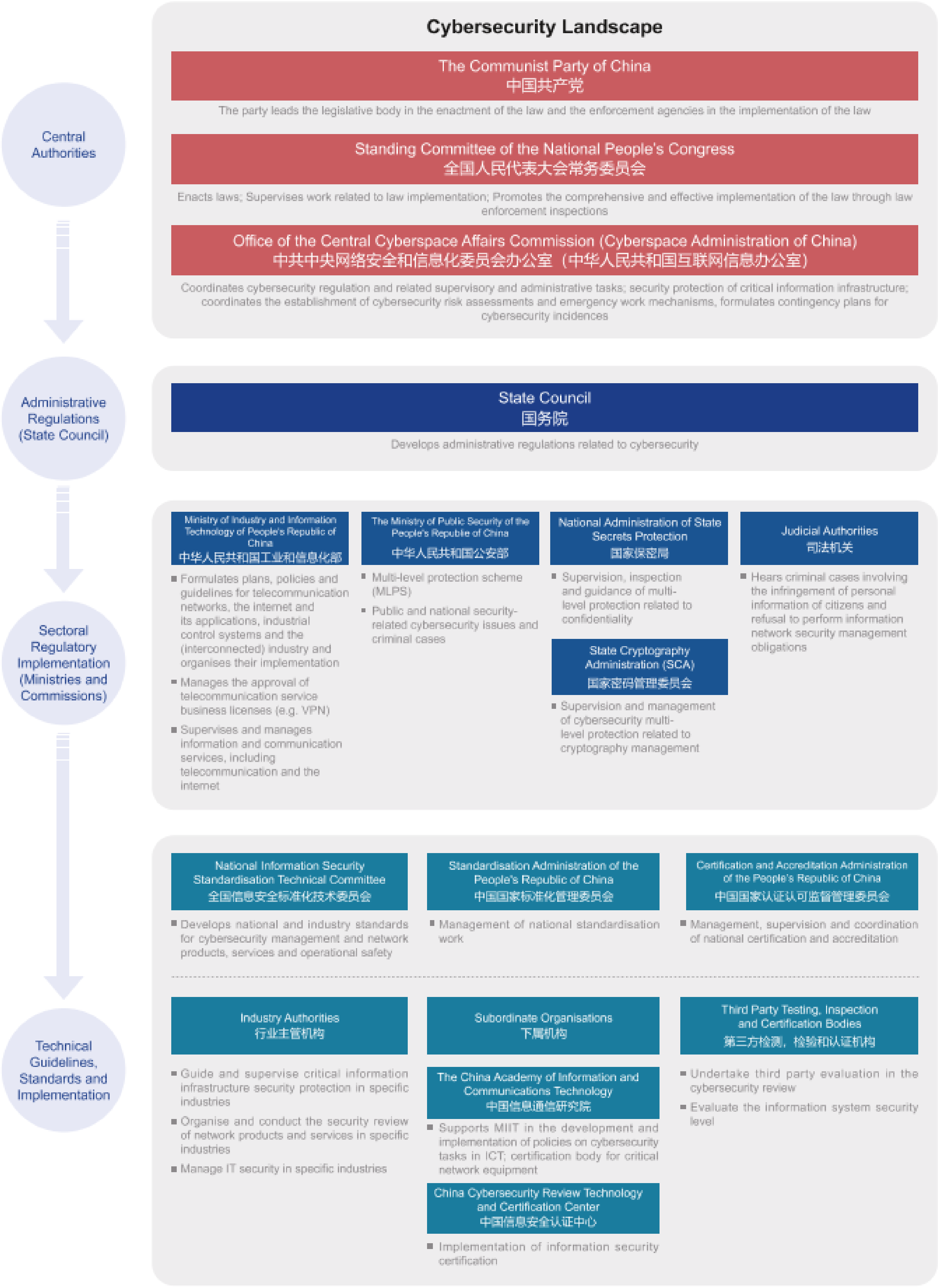
Coming into effect on June 1st 2017, the Cybersecurity Law forms the basic legal framework for cybersecurity and data protection in China. It categorises cyberspace resources and activities according to their risk and sensitivity, as well as establishes corresponding compliance requirements. The law systemised a number of pre-existing regulatory measures and acts as an umbrella document which will be continually supported by a series of implementing regulations, rules and guidance. Its key components consist of :

- Generic cybersecurity requirements for “Network Operators”;
- Regulations on Personal Information and Important Data protection;
- Special requirements for Critical Information Infrastructure Operators (CIIOs);
- Regulations on data localisation and cross-border data transfer;
- Compulsory certification and security reviews on network products and services;
- Internet content management;
- Multi-level Protection Scheme (MLPS).

Various regulatory authorities play different and sometimes overlapping roles in the field of cybersecurity. These authorities include the Cyberspace Administration of China (CAC), State Council, Ministry of Industry and Information Technology (MIIT), Ministry of Public Security (MPS), the National Information Security Standardisation Technical Committee (TC260), among others.

The CAC was established in 2014 and has been central to the development of China’s cybersecurity framework, having released some of the key laws and regulations over the last few years. The MIIT has played a key role in developing industrial policies and standards in China’s ICT sector. While the MPS, China’s main security and intelligence agency, is responsible for protecting the country from security attacks, as well as overseeing the Multi-Level Protection System (more information below). TC260 is jointly run by CAC and MIIT, and has issued the majority of technical standards in the cybersecurity field.

The regulatory system of cybersecurity in China is as follows:



Cybersecurity Landscape

Central Authorities

The Communist Party of China
中国共产党

The party leads the legislative body in the enactment of the law and the enforcement agencies in the implementation of the law

Standing Committee of the National People's Congress
全国人民代表大会常务委员会

Enacts laws; Supervises work related to law implementation; Promotes the comprehensive and effective implementation of the law through law enforcement inspections

Office of the Central Cyberspace Affairs Commission (Cyberspace Administration of China)
中共中央网络安全和信息化委员会办公室（中华人民共和国互联网信息办公室）

Coordinates cybersecurity regulation and related supervisory and administrative tasks; security protection of critical information infrastructure; coordinates the establishment of cybersecurity risk assessments and emergency work mechanisms, formulates contingency plans for cybersecurity incidences

Administrative Regulations (State Council)

State Council
国务院

Develops administrative regulations related to cybersecurity

Sectoral Regulatory Implementation (Ministries and Commissions)

Ministry of Industry and Information Technology of People's Republic of China
中华人民共和国工业和信息化部

- Formulates plans, policies and guidelines for telecommunication networks, the internet and its applications, industrial control systems and the (interconnected) industry and organises their implementation
- Manages the approval of telecommunication service business licenses (e.g. VPN)
- Supervises and manages information and communication services, including telecommunication and the internet

The Ministry of Public Security of the People's Republic of China
中华人民共和国公安部

- Multi-level protection scheme (MLPS)
- Public and national security-related cybersecurity issues and criminal cases

National Administration of State Secrets Protection
国家保密局

- Supervision, inspection and guidance of multi-level protection related to confidentiality

State Cryptography Administration (SCA)
国家密码管理委员会

- Supervision and management of cybersecurity multi-level protection related to cryptography management

Judicial Authorities
司法机关

- Hears criminal cases involving the infringement of personal information of citizens and refusal to perform information network security management obligations

Technical Guidelines, Standards and Implementation

National Information Security Standardisation Technical Committee
全国信息安全标准化技术委员会

- Develops national and industry standards for cybersecurity management and network products, services and operational safety

Standardisation Administration of the People's Republic of China
中国国家标准化管理委员会

- Management of national standardisation work

Certification and Accreditation Administration of the People's Republic of China
中国国家认证认可监督管理委员会

- Management, supervision and coordination of national certification and accreditation

Industry Authorities
行业主管机构

- Guide and supervise critical information infrastructure security protection in specific industries
- Organise and conduct the security review of network products and services in specific industries
- Manage IT security in specific industries

Subordinate Organisations
下属机构

The China Academy of Information and Communications Technology
中国信息通信研究院

- Supports MIIT in the development and implementation of policies on cybersecurity tasks in ICT; certification body for critical network equipment

China Cybersecurity Review Technology and Certification Center
中国信息安全认证中心

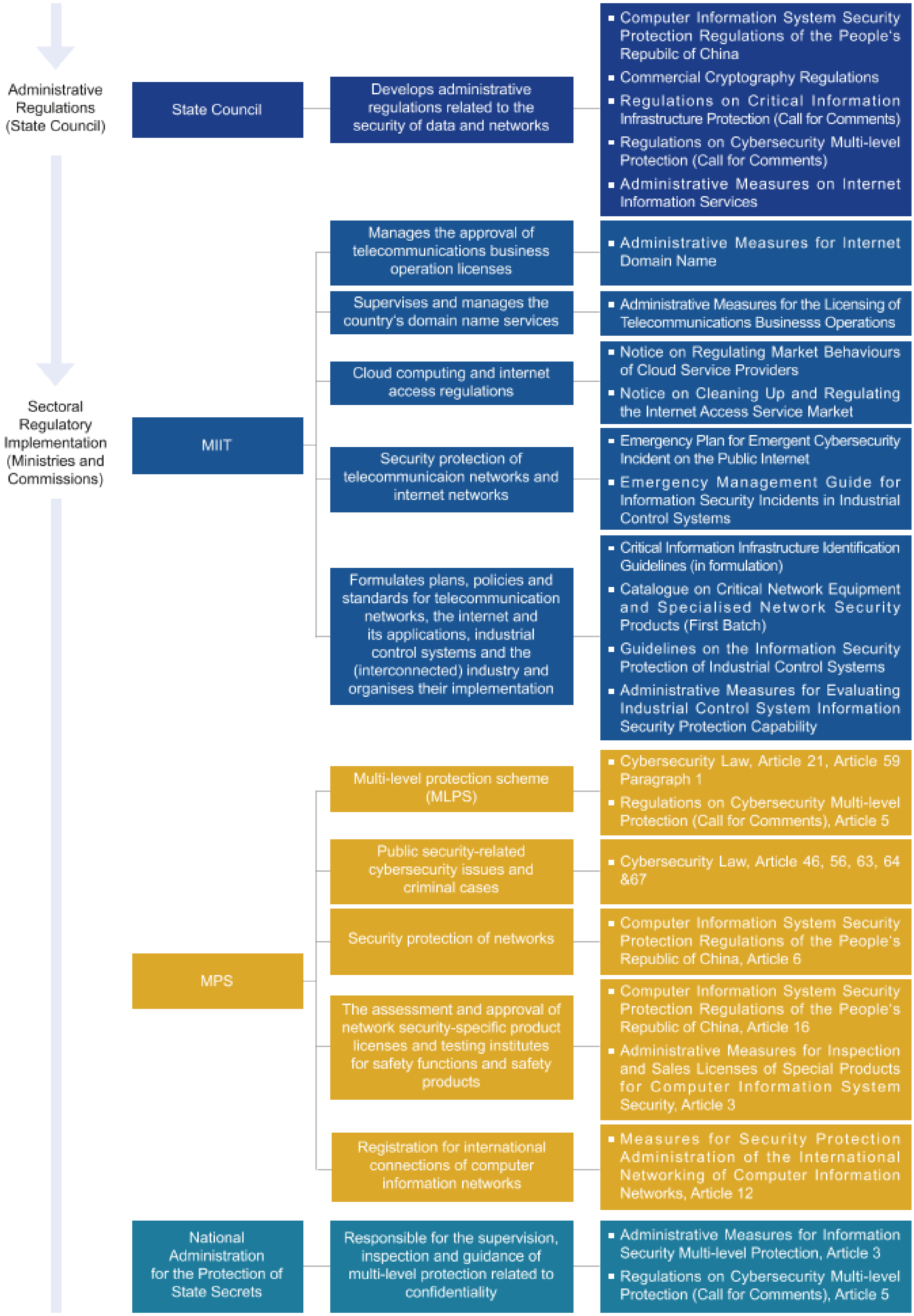
- Implementation of information security certification

Third Party Testing, Inspection and Certification Bodies
第三方检测，检验和认证机构

- Undertake third party evaluation in the cybersecurity review
- Evaluate the information system security level

A detailed outline of their respective functions and legislative actions are represented in the chart below:

Central Authorities		
CAC	Coordinates cybersecurity work and related supvervisory and management tasks	▪ Cybersecurity Law, Article 8 ▪ Regulations on Cybersecurity Multi-level Protection (Call for Comments), Article 5 ▪ National Cyberspace Security Strategy
	Supervises and manages network information security	▪ Cybersecurity Law, Article 50 & 68 ▪ Regulations on Internet Content Management Administration Law Enforcement Procedures, Article 2&4 ▪ Provisions for the Administration of Internet Information Services ▪ Implemening Rules on the Licensing of Internet News Information Services ▪ Administrative Provisions on Internet Post Comments Services ▪ Administrative Provisions on Internet Forum Community Services ▪ Administrative Provisions on Internet Group Information Services ▪ Administrative Provisions on Internet User Public Account Information Services
	Coordinates the security protection of critical information infrastructure	▪ Telecommunications Regulations of the People's Republic of China, Article 27, 28, 29 & 30 ▪ Guidelines for the Operation of National Cybersecurity Inspections ▪ Critical Information Infrastructure Identification Guidelines (under formulation)
	Protects personal information and important data	▪ Cybersecurity Law, Article 64, Paragraph 1 ▪ Data Security Management Measures(Draft)
	Develops and publishes a catalogue for critical network equipment and special network security products	▪ Cybersecurity Law, Article 23 ▪ Catalogue on Critical Network Equipment and Specialised Network Security Products (First Batch) ▪ Notice on the Publication of the Directory of Internet Key Equipment and Cybersecurity-specific Product Safety Certifications and Safety Test Mechanisms (First Batch)
	Organises national security reviews of network products and services	▪ Cybersecurity Law, Article 35 ▪ Security Review Measures for Network Products and Services(trial implementation), Article 5 ▪ Measures for Cybersecurty Review (Draft)
	Coordinates the security assessment of cross-border data transfers	▪ Cybersecurity Law, Article 37 ▪ Measures on the Security Assessment of Cross-border Transfer of Personal Information and Important Data (Call for Comments) ▪ Measures on Security Assessment for Cross-border Transfer of Personal Informabion (Draft) ▪ Data Secunty management Measures (Draft)
	Coordinates the collection, analysis and notification of cybersecurity information	▪ Cybersecurity Law, Article 51
	Coordinates the establishment of cybersecurity risk assessments and emergency work mechanisms, formulates contingency plans for cybersecurity incidences	▪ Cybersecurity Law, Article 53 ▪ Emergency Plan for National Cybersecurity Incidents



Administrative Regulations (State Council)	State Council	Develops administrative regulations related to the security of data and networks	▪ Computer Information System Security Protection Regulations of the People's Repubilc of China ▪ Commercial Cryptography Regulations ▪ Regulations on Critical Information Infrastructure Protection (Call for Comments) ▪ Regulations on Cybersecurity Multi-level Protection (Call for Comments) ▪ Administrative Measures on Internet Information Services
Sectoral Regulatory Implementation (Ministries and Commissions)	MIIT	Manages the approval of telecommunications business operation licenses	▪ Administrative Measures for Internet Domain Name
		Supervises and manages the country's domain name services	▪ Administrative Measures for the Licensing of Telecommunications Businesss Operations
		Cloud computing and internet access regulations	▪ Notice on Regulating Market Behaviours of Cloud Service Providers ▪ Notice on Cleaning Up and Regulating the Internet Access Service Market
		Security protection of telecommunicaion networks and internet networks	▪ Emergency Plan for Emergent Cybersecurity Incident on the Public Internet ▪ Emergency Management Guide for Information Security Incidents in Industrial Control Systems
		Formulates plans, policies and standards for telecommunication networks, the internet and its applications, industrial control systems and the (interconnected) industry and organises their implementation	▪ Critical Information Infrastructure Identification Guidelines (in formulation) ▪ Catalogue on Critical Network Equipment and Specialised Network Security Products (First Batch) ▪ Guidelines on the Information Security Protection of Industrial Control Systems ▪ Administrative Measures for Evaluating Industrial Control System Information Security Protection Capability
	MPS	Multi-level protection scheme (MLPS)	▪ Cybersecurity Law, Article 21, Article 59 Paragraph 1 ▪ Regulations on Cybersecurity Multi-level Protection (Call for Comments), Article 5
		Public security-related cybersecurity issues and criminal cases	▪ Cybersecurity Law, Article 46, 56, 63, 64 &67
		Security protection of networks	▪ Computer Information System Security Protection Regulations of the People's Republic of China, Article 6
		The assessment and approval of network security-specific product licenses and testing institutes for safety functions and safety products	▪ Computer Information System Security Protection Regulations of the People's Republic of China, Article 16 ▪ Administrative Measures for Inspection and Sales Licenses of Special Products for Computer Information System Security, Article 3
		Registration for international connections of computer information networks	▪ Measures for Security Protection Administration of the International Networking of Computer Information Networks, Article 12
	National Administration for the Protection of State Secrets	Responsible for the supervision, inspection and guidance of multi-level protection related to confidentiality	▪ Administrative Measures for Information Security Multi-level Protection, Article 3 ▪ Regulations on Cybersecurity Multi-level Protection (Call for Comments), Article 5

	State Cryptography Administration	Responsible for the supervision and management of cybersecurity classified proection works related to cryptography management	▪ Cryptography Law of the People's Republic of China (Draft Call for Comments), Article 5 ▪ Commercial Cryptography Regulations, Article 4 ▪ Administrative Measures for Information Security Multi-level Protection, Article 29 ▪ Regulations on Cybersecurity Multi-level Protection (Call for Comments), Article 5
Technical Guidelines and Standards	TC260	Develop national and industry standards for cybersecurity and network products and services	▪ Information Security Technology – Guidelines for Data Cross-Border Transfer Security Assessment (Call for Comments) ▪ Information Security Technology – Guide to Security Inspection and Evaluation of Critical Information Infrastructure (Call for Comments) ▪ Information Security Technology – Indicator System of Critical Information Infrastructure Assurance (Call for Comments) ▪ Information Security Technology – Cybersecurity Protection Requirements of Critical Information Infrastructure (Call for comments) ▪ Information Security Technology – Personal Information Security Specification (GB/T 35273-2017) ▪ Information Security Technology – Security Impact Assessment Guide of Personal Information (Call for Comments) ▪ Information Security Technology – Guidelines for Personal Information De-identification (Call for Comments) ▪ Information Security Technology – Guideline for Personal Information Protection within Information Systems for Public and Commercial Services ▪ Information Security Technology – Implementation Guide for Cybersecurity Classified Protection (Call for Comments) ▪ Information Security Technology – Guidelines for Grading of Classified Protection of Cybersecurity ▪ Information Security Technology – Testing and Evaluation Process Guide for Cybersecurity Classified Protection (Call for Comments) ▪ Information Security Technology – Testing and Evaluation Technology Guide for Cybersecurity Classified Protection (Call for Comments) ▪ Information Security Technology – Big Data Security Management Guide (Call for Comments) ▪ Information Security Technology – Evaluation Measures for the Security Capability of Cloud Computing Services ▪ Information Security Technology – General Security Requirements for Network Products and Services (Call for Comments) ▪ Conditions and Code of Conduct for Information Technology Products Safety Inspection Bodies (Call for Comments)

Part Ⅲ

Compliance Suggestions for British Business

According to our survey, UK companies have confronted challenges in dealing with the law, in particular on 1) Personal information; 2) Important data; 3) Data localisation and cross-border data transfer and 4) the Multi-level protection scheme (MLPS). Below, we provide a brief explanation, as well as some recommendations for UK companies. Owing to the scale and complexity of such requirements, professional services firms are often consulted for specific compliance advice.

3.1 Compliance with Personal Information Protection Requirements

To determine whether a UK company must comply with the Personal Information protection requirements, the first step is to identify whether the data collected or processed by the UK company falls into the scope of Personal Information.

Step I: Data Identification

Personal Information is defined as various types of information recorded in an electronic format or otherwise that can be used separately or in combination with other information to identify a natural person, including but not limited to the name, date of birth, identity certificate number, personal biological identification information, address, telephone numbers, etc. of the natural person (see the CSL article 76).

Coming into effect in May 2018, GB/T 35273-2017 Information Security Techniques - Personal Information Security Specification (the "Personal Information Specification"), published by the National Information Security Optimisation Technical Committee of China (the "ISSC") provides more detailed examples of Personal Information. The key factor to identify whether the data falls into the scope of Personal Information is whether the company has the ability to use such data to identify natural persons (i.e. data subjects).

Step II: Review the Legal Basis of Personal Information Processing Activities

Personal Information processing activities include collection, storage, use, sharing, deletion, transfer, public disclosure, user profiling, personalise display, etc. Unlike the European General Data Protection Regulations (GDPR), the legal basis of Personal Information processing activities under the CSL are entirely consent-based.[2] Network Operators shall comply with the following requirements:

- Comply with the principles of legality, justification and necessity;
- Publicise the rules for Personal Information processing and clearly indicate the purposes, methods and scope of data collection and use;
- Obtain the consent of those from whom the information is collected (i.e. Personal Information subjects);
- Any processing activities shall be carried out within the scope of the consent;
- A renewed consent is required when the processing exceeds the original scope of consent;
- Seek explicit consent from children's guardians prior to collecting or using children's Personal Information in cases where the minors are aged under 14.

[2] Chapter 6 of the GDPR requires any organisation processing personal data to have a valid legal basis for that personal data processing activity. The GDPR provides six legal bases for processing, namely 1) Consent; 2) Performance of a Contract; 3) Legitimate Interest; 4) Vital Interest; 5) Legal Requirement; 6) Public Interest

For UK companies which process Personal Information in China, it is important to conduct a full compliance due diligence of the legal basis of data processing and optimise the authorisation documents of the Personal Information subjects.

Step III: Policy optimisation of the Rights of Personal Information Subjects

The CSL entitles a series of rights of personal information subjects, supplemented by the national standard "Personal Information Specification", including rights to deletion, rectification, access, withdrawal of consent, cancelation of accounts, and request for copies.

To comply with these requirements, it is recommended for UK complies to conduct gap analysis on data processing activities to determine if the company has clearly notified Personal Information subjects of their rights, and whether there are effective mechanisms in place so they can exercise these rights in an efficient way.

3.2 Compliance with Important Data Protection Requirements

To determine whether a UK company must comply with the Important Data protection requirements, the first step is to identify whether the data collected or processed by the UK company falls into the scope of Important Data.

Definition of Important Data

Important Data is generally perceived as data that is closely related to national security, economic development and public interest[3]. Examples of Important Data include unpublished government information, and a large volume of data relating to population, genetics, healthcare, or geographical and mineral resources[4], usually excluding the operational and corporate administration data of businesses and personnel information.

To understand the specific scope of Important Data is critical because onerous requirements such as data localisation and security assessments for cross-border transfer are attached to Important Data. However, the implementing regulations and national standards on Important Data are still being drafted and there is no definite scope of Important Data yet.

Important Data protection requirements are still open to change

Administrative Measures on Data Security (Draft, 2019) released on 28 May 2019 proposes some new requirements, containing a special focus on the protection of important data.

Risk Assessment- Network Operators shall assess the potential security risks prior to releasing, sharing or selling Important Data or transferring such data abroad.

Filing records- Network Operators are also required to file records with local cyberspace administrations for collecting Important Data within China for business purposes, which shall include the rules for collection and use of such data, purposes, scales, methods, scopes, types and retention periods of the data, but will not include the contents of data. However, the filing process is still unclear and further guidance is expected to be released by the government;

It should be noted that the Administrative Measures on Data Security (Draft, 2019) is still open to change. Once it is finalised, we expect to have clarity on a number of issues such as the methodology of the security assessment and the scope of Important Data.

[3] Measures for Security Assessment of Cross-Border Transfer of Personal Information and Important Data (Draft) .2017

[4] Administrative Measures on Data Security (Draft).2019

3.3 Internal Management Measures of Data Protection

Taking account of the CSL, related regulations and industry experience, the following measures are recommended for UK companies.

- Localisation - The GDPR in the EU and the CSL in China have large differences. Compliance with GDPR requirements does not guarantee compliance with the CSL. Companies should actively localise global data security policies and management measures to ensure that local policies in China meet the legislative gaps between the EU and China.
- Personnel - Formulate internal security management systems and operation instructions to determine the person in charge of cyber security (including data security, data protection and other cyber security requirements) and define the corresponding accountabilities;
- Preparation - Take technical and other necessary measures to ensure data security, and to protect such data from disclosure, damage or loss;
- Contingency planning - Formulate a contingency plan for data security incidents and deal with security risks such as system vulnerabilities, computer viruses, cyberattacks and cyber intrusions in a timely manner. In the case of actual or potential disclosure, damage or loss of Personal Information, UK companies shall take remedial measures, notify the Personal Information subjects and report the matter to the competent authorities in accordance with the relevant provisions;
- Review and update - Many of the CSL's implementing measures are still in draft form. Review and improve the data compliance and contingency planning system on a regular basis to ensure that they are up to date;
- Training - Conduct routine internal training to ensure security at all levels.

3.4 Data Localisation and Cross-border Data Transfer

As revealed by the online survey, cross-border data transfer and data localisation are key issues for UK companies in China. In its current form, the CSL requires that Personal Information and Important Data collected by critical information infrastructure operators ("CIIOs") shall be stored within China ("Data Localisation Requirement"). Critical information infrastructure refers to information facilities that directly concern national security and stability and may seriously endanger national security and public interest. While further implementing regulations are expected, the sectors that have been explicitly named include energy, finance, transportation, education, scientific research, water conservancy, industrial manufacturing, healthcare, social security and public utilities. Where it is necessary to export Personal Information and Important Data collected by CIIOs abroad due to business needs, a security assessment shall be carried out.

However, since 2017 the Cyberspace Administration of China ("CAC") has published a series of draft implementing measures of the CSL including *Measures for Security Assessment of Cross-border Transfer of Personal Information and Important*

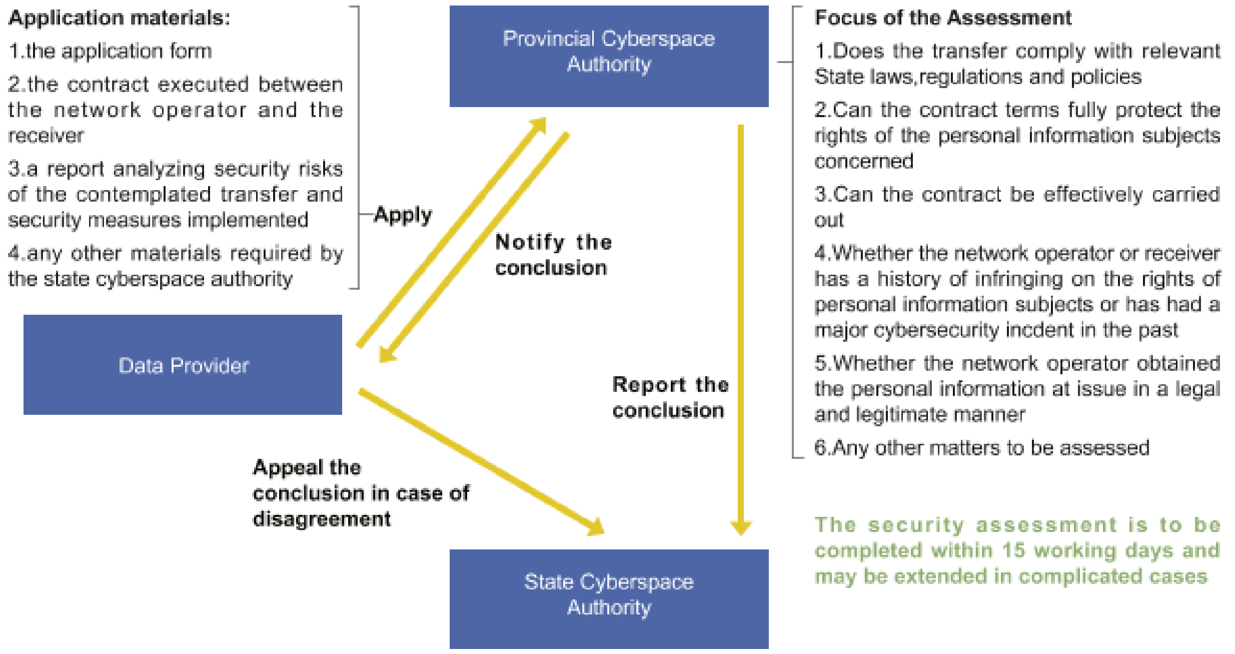
Data (Draft, 2017), Administrative Measures on Data Security (Draft, 2019), and Measures on Security Assessment for Cross-border Transfer of Personal Information (Draft, 2019).

At present, these cross-border data transfer regulations have not come into force. For UK companies, it is nonetheless important to pay close attention to these developments, which reveal a few key shifts in the regulator's attitude to cross-border data transfer:

- The scope of entities to which data export restrictions may apply has been significantly expanded from CIIOs to each **Network Operator**. Arguably, any entity in China that uses computer systems connected to communication networks would be considered a Network Operator, and therefore would be subject to the security assessment requirements.
- Prior to the cross-border transfer of **Personal Information**, Network Operators shall apply to the local cyberspace administrations at the provincial level for security assessment, file an application form, the data processing agreement signed between the company and data receivers, an analysis report on the security risks for the cross-border transfer of Personal Information and security measures and other materials required (if any).[5]
- For cross-border transfer of **Important Data**, if the draft measure is adopted in its current form, UK companies will be required to file records with authorities for the collection of Important Data, conduct a security assessment and obtain the approval of authorities prior to the cross-border transfer of Important Data or any kind of Important Data processing activities.[6]

Moreover, we set out the procedure for such security assessment of Cross-border Transfer of Personal Information under the current draft measures to show the whole picture of the regulation of cross-border data transfer in China.

Security Assessment Process for Cross-border Transfers of Personal Information



Application materials:

1.the application form

2.the contract executed between the network operator and the receiver

3.a report analyzing security risks of the contemplated transfer and security measures implemented

4.any other materials required by the state cyberspace authority

Apply
Provincial Cyberspace Authority
Notify the conclusion
Data Provider
Report the conclusion
Appeal the conclusion in case of disagreement
State Cyberspace Authority

Focus of the Assessment

1.Does the transfer comply with relevant State laws,regulations and policies

2.Can the contract terms fully protect the rights of the personal information subjects concerned

3.Can the contract be effectively carried out

4.Whether the network operator or receiver has a history of infringing on the rights of personal information subjects or has had a major cybersecurity incdent in the past

5.Whether the network operator obtained the personal information at issue in a legal and legitimate manner

6.Any other matters to be assessed

The security assessment is to be completed within 15 working days and may be extended in complicated cases

[5] Measures on Security Assessment for Cross-border Transfer of Personal Information (Draft, 2019), Articles 3 & 4.

[6] Administrative Measures on Data Security (Draft), Article 28

At present, the specific scope of Important Data and the procedure for such security assessment of cross-border data transfer remain unclear. However, UK companies are recommended to review their data flows, segment them into categories, and closely monitor the latest legislative developments.

3.5 Multi-level Protection Scheme (MLPS)

The Multi-Level Protection Scheme ("MLPS") for cybersecurity is a tiered information security protection system established within the CSL framework. The draft implementing regulations8[7] published in 2018 and the recent roll-out in May 2019 of national standards[8], referred to as "MLPS 2.0", implements security management requirements in relation to a company's cybersecurity protection system. Due to come into force nationwide in December 2019, the MLPS 2.0 is stricter and broader than its predecessor.

Subjects

The MLPS is required to be applied society-wide by all regional governments, agencies and departments, enterprises and institutions on networks and systems located within China. These include all networks[9] except for self-built personal or home networks intended for self-use. The MLPS stipulates general technical and institutional requirements for all networks/systems along with some specific requirements for key applications including information network infrastructures, cloud computing platforms/systems, Big Data applications/platforms/resources, the Internet of Things (IoT), industrial control systems, and systems using mobile internet technology.

Subject Identifications

All networks/systems are divided into five levels of protection based on the degree of risk and importance, from Level I to Level V. For every level, there are different protection identification principles (set out in Appendix III: Identifications of the MLPS and related protection obligations.

Steps for UK Companies to Conduct the MLPS

Step Ⅰ
Subject Identifications

Step Ⅱ
Self - evaluation with a written justification

Step Ⅲ
Expert examination

Step Ⅳ
Authorities examiination and approval

Step Ⅴ
Filing with Public Security Organs

[7] The Ministry of Public Security published the Regulations on the Classified Protection of Cybersecurity (Draft) on June 27, 2018.

[8] GB/T 22239 – 2019 Information Security Technology – Baseline for Multi-level Protection Scheme, GB/T 25070 – 2019 Information Security Technology – Technical Requirements of Security Design for Multi-level Protection Scheme and GB/T 28448 – 2019 Information Security Technology – Evaluation Requirements for Multi-level Protection Scheme.

[9] Network here includes not only user-oriented websites, platforms, apps, mobile networks, e-commerce platforms and cloud platforms, but also information systems that support corporate services, such as communication facilities, industrial control systems, and office and business management systems.

- Steps 1 & 2: All Network Operators should conduct a **self-evaluation** to determine the level to which their networks/systems belong.
- Step 3: For Level II or above, companies shall organise an **expert review** and **file a record** with the public security organs.
- Step 4: The public security organs will examine the materials submitted by the company for record-filing purposes.
- Step 5: Where the network/system is graded appropriately and the record-filing materials provided meet the relevant requirements, the public security organ will issue a **record-filing certificate** of the MLPS.

Once the level of network/systems has been determined, Network Operators should comply with the corresponding requirements, as well as additional requirements that pertain to information network infrastructures, cloud computing platforms/systems, Big Data applications/platforms/resources, the Internet of Things (IoT), industrial control systems, and systems using mobile internet technology.

Obligations of the MLPS

Under the MLPS, there are different obligations for each level of networks/systems. Except for the general requirements for all levels of networks/systems, there are some specific additional requirements for Level III and above. In particular, it is required that networks/systems at or above Level III shall be technically maintained within the territory of China, and remote technical maintenance from overseas is prohibited. Where it is truly necessary to have networks/systems technically maintained remotely from overseas, it shall be required to conduct the cybersecurity review. However, the details of such review have not been published yet.

To better understand the whole picture of obligations for UK companies as network operators under the MLPS, we set out the general requirements along with the additional requirements for networks at or above Level III in Appendix IV.

Moreover, UK companies in China are recommended to pay close attention to the regulatory requirements of the competent administrative authorities, strengthen mechanisms of communications with administrative and cyberspace administration authorities, and implement multi-level protection on their networks/systems.

Part Ⅳ Expert Insights

To better understand the legal framework and relevant practice of cybersecurity and data protection in the Chinese market and provide advice to UK companies on how to deal with potential challenges, we consulted some experts from Chinese authoritative institutions and relevant representatives of Chinese and UK companies.

An Interview with Prof. Ke Xu, Executive Director of UIBE's Digital Economy and Legal Innovation Research Center

Keywords: Law Enforcement Coordination, CIIO, GDPR

Ke Xu

Prof. Ke Xu is the Executive Director of UIBE's Digital Economy and Legal Innovation Research Center and the Deputy Director of the Fintech and Cyber Security Research Center of Renmin University.

Prof. Xu received his PhD in Law from UIBE and was in the CSC/UC Visiting Researcher Fellowships Program jointly sponsored by the Chinese Ministry of Education and UC Berkeley. Before attending Renmin University, he practiced corporate and banking law in a leading law firm for several years.

In May 2019, we invited Prof. Xu to provide a systematic introduction on the legal framework of cybersecurity in China. The insights he relayed were both based on his own expert observations, as well as conversations with relevant Chinese government officials.

Overarching legal framework

As discussed by Prof. Xu, the legal system of cybersecurity laws in China consists of many levels. Sorted by level of effectiveness, from high to low, we have "laws", "administrative regulations" and "national standards".

The ministries and commissions related to cybersecurity legislation at "administrative regulations" level include the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology (MIIT) and the Ministry of Public Security (MPS). Currently, many of the CSL's implementation rules and technical standards remain in draft form. Prof. Xu emphasised the importance for UK companies to establish communication channels with the policy and regulations bureau of the CAC and MIIT by either submitting internal reference documents or attending their seminars.

Regulatory responsibilities

As to the respective powers of these authorities, we have observed that the phenomenon of "Nine Dragons Controlling Water" still exists in the cybersecurity area, indicating the multiple regulatory authorities involved in the cybersecurity realm. For example, the CAC focuses on the control of CII, data localisation, and cross-border data transfer; while the MIIT focuses on the perspective of industrial development and the MPS oversees the Multi-level Protection Scheme (MLPS) and advocates that this system is the basis for protecting the CII, and therefore the MPS has the power to regulate the CIIO. Prof. Xu believes that what the CAC can do is probably act as a policy coordinator and issuer.

"The current trend is that the CAC is tending to position itself as the leading authority for personal information protection, but this positioning is not yet agreed upon by the other authorities. So, which of the authorities will be in charge of personal information protection in the future is yet to be determined by the Personal Information Protection Law (a draft of which will be released this year according to the current legislative plan)".

Regarding the "national standards", they are very significant to guiding national regulatory criteria and corporate compliance. UK companies are encouraged to comply with these standards, even those that are not yet mandatory from being cited in laws or regulations.

Moreover, on the CIIO front, Prof. Xu said that the detailed implementation rules of the CII are still missing at the legislative level. The Chinese legislature conducted field research in "BAT" (i.e., Baidu, Alibaba and Tencent) and other big internet companies, but it has never explicitly said which companies are CIIOs.

An Interview with Prof. Shenkuo Wu, Senior Advisor of the United Nations Network Security and Cybercrime

Keywords: Administrative Measures on Data Security (Draft), Measures for Cybersecurity Censorship (Draft), GDPR Enforcement, Good Compliance Practices

Shenkuo Wu

Professor Shenkuo Wu is Director of the International Centre of Cyber Law of Beijing Normal University.

He is a leading expert on Chinese cybersecurity law, data protection and the law of cybercrime. He acts as a senior consultant of the United Nations as well as of the Supreme People´s Court of the People´s Republic of China. Prof. Wu also heads the Research Centre of the Internet Society of China.

In June 2019, the Cyberspace Administration of China (CAC) released three Exposure Drafts within 10 days of each other. With this in mind, we invited Prof. Wu to share his insights into these latest developments.

According to Professor Wu, legislative work will be divided into two main categories:

- The construction of top-level design, including personal information protection and data security laws;
- The development of specific rules around cross-border data transfer, and adapting the law to

specific industry sectors, such as medical, tax, customs, as well as new technologies such as facial recognition.

In short, there will be some new rules in macro top-level design, micro-sectors, industries, and even specific technology application scenarios.

Since there are still some policies yet to be released, the gap between legislation and enforcement will pose certain challenges to companies. Professor Wu also gives some suggestions in terms of best practices for British companies in China.

Supply chain transparency

The first is the issue of system operation security, which means a voluntary display of supply chain transparency, instead of waiting for regulators to come and carry out their own investigations. Now what regulators want to see is not how good your firewall or your antivirus program is, but whether you can reliably demonstrate every stage of your supply chain from beginning to end for your network products and services.

The need to adjust to China's specific requirements

The other "red-line" issue concerns where you stand when it comes to data security. In this respect, many foreign companies tend to still go by a global strategy for the Chinese part of their business, and are slow to adapt to the local environment. China is currently at the early stage of creating a data security regime and is undergoing drastic changes in this respect, so foreign companies should keep track of the relevant regulatory developments on data security. Since many other authorities will publish regulations in their respective fields, UK companies in China should pay attention to keeping track of and understanding these regulations in a timely and systematic way.

The last suggestion is to avoid such misconception that "I have met certain overseas standards and the Chinese standards can't be stricter, so naturally I should also be in compliance with the Chinese standards". Companies will still need to check their compliance in China frequently. **This is not asking UK companies in China to instantly change their way of management. It's just suggesting that they should express their way of management in a more local, Chinese way.**

An Interview with Mr. Donald Wang, Senior Legal Counsel of Sina Corporation

Keywords: Privacy by Design, GDPR and China's Cybersecurity Law

Industry: Internet

Donald Wang

Mr. Donald Wang is senior legal counsel from Sina.com technology (China) Co., LTD.

He created Sina's policy research team and serves as an expert member in various industry associations, such as the United Nations Committee of E-commerce, the Beijing Association of Investment Expert and the Legal Work Committee of the Internet Society Network Information Office. He has good relationships with government agencies and various regulators, such as the MOFCOM, etc.

Mr. Wang shared with us that the focus on data is a global consensus at present – **data is the new oil**. In his communication with experts from the European Union and the United States, it turns out that it is equally difficult for them to determine what specific practices are acceptable from a compliance perspective. Both countries mentioned a concept called "**dynamic compliance**", according to which the circumstances of data use may change at any time. Facing these challenges, Mr. Wang provides his perspective on the best practices of **data collection and processing**.

The first is giving data subjects (i.e. users of platforms) certain rights of choice through some functional designs. This is also called "**Privacy by Design**", which allows users to revoke consent and unregister themselves.

The second is **informing and obtaining the consent** of users when collecting information and being as clear as possible with the purpose of collecting the information. Trying to simplify the functions of apps to inform users before they proceed to the legal terms is a good practice to follow. In the subsequent use of the information collected, some principles must also be followed. Not jeopardising national security and territorial integrity and sovereignty is the first and foremost requirement.

In addition, regarding user consent to collect, process and use personal information, there should be an overall judgment and framework, as well as corresponding remedies.

For some multinational companies that are facing regulation from both the GDPR and China's Cybersecurity Law, Mr. Wang also shared his opinion about the similarities and differences between the GDPR and China's Cybersecurity Law.

The provisions of the GDPR are more dynamic and account for exceptions, whilst China's Cybersecurity Law is relatively static and needs to be supported and supplemented with further efforts. But both the GDPR and China's Cybersecurity Law share the same objectives, that is, to protect users' personal information, facilitate efficient flow of data, and fully recognise the value of the relevant data.

An Interview with Mr. Baoqiu Cui, Vice President of Xiaomi Corporation

Keywords: Definition of personal data, Privacy protection committee, Five Principles for Privacy Protection

Industry: Innovative Technology Enterprise

Baoqiu Cui

Mr. Baoqiu Cui, Vice President of Xiaomi Corporation, Chairman of Technical Committee

Mr. Cui is the former Chief Architect of Xiaomi and Vice President of AI and Cloud Platform

To some extent, the value of big data and user privacy is contradictory. From the perspective of maximising the value of big data and without prejudice to the interests of all parties, the more data that is shared, exchanged and mined, the higher the value that will be generated. However, from the perspective of security and privacy, every individual demands privacy and no user wants their privacy compromised. Therefore, we need to find a balance between making the most out of big data whilst respecting the privacy of our users at the same time.

"Currently, there are multiple definitions of 'Personal Information'. **The definition of Singapore's Personal Data Protection Commission (PDPC) is a relatively strict one. Personal Information is defined as data, whether true or not, about an individual who can be identified from that data and other information to which the organisation has or is likely to have access."**

"Xiaomi were pioneers in privacy protection by setting up a privacy protection committee, carrying out privacy training and conducting privacy certification," Mr. Cui said. When it comes to privacy protection, Xiaomi put forward five principles.

The first is to inform and acknowledge. To collect users' data, it is necessary to tell the users the nature of the company collecting the data and the reason for doing so. **Privacy is a spectrum and there are no absolute black and white guarantees when it comes to privacy protection. Therefore, when we have uncertainties, what we can do is inform the users and assure them to the largest extent possible**.

The second principle is options and consent, that is, to inform the users and obtain their consent.

The third principle is the users' control and participation. It is possible that the users may forget the names of companies that collect their information and the content of such information over a period of time. Therefore, we need to let the users see what data has been collected and give them the right to modify their privacy options and amend the data itself.

The fourth principle is data integrity and security. The data must be encrypted during the uploading and storage process. During data processing, data desensitisation must be conducted if necessary. Meanwhile, access control in regards to both technology and data management should be implemented.

The fifth principle is mandatory measures and remedies. It is important to obtain certification from an external privacy certification company. **When developing a new product, from the outset it is necessary to think about the issues of respecting user privacy, including what data should or should not be collected, whether it is necessary to inform the user, how to obtain the user's consent without affecting the user experience, etc.**

Appendix I: Legal Definitions

Term	Definition	Reference

Personal Information	"Personal Information" is defined as various types of information recorded in an electronic format or otherwise that can be used separately or in combination with other information to identify a natural person, including but not limited to the name, date of birth, identity certificate number, personal biological identification information, address, telephone numbers, etc. of the natural person.	Cybersecurity Law of the PRC;
		Information Security Technology - Personal Information Security Specification (GB/T 35273-2017);
		Measures for Security Assessment of Cross-border Transfer of Personal Information (Draft)

Important data	"Important Data" is generally perceived as data that is closely related to national security, economic development and public interest. Examples of Important Data include unpublished government information, and a large volume of data relating to population, genetics, healthcare, or geographical and mineral resources.
	The implementing regulations and national standards on Important Data are still being drafted and there is no definite scope of Important Data yet.
		Measures for Data Security Management (Draft, 2019);
		Measures for Security Assessment of Cross-border Transfer of Personal Information and Important Data (Draft, 2017);
		GB/T-Information Security Technology - Guidelines for Data Cross-border Transfer Security Assessment (Draft)

Network Operators	"Network Operators" are defined as owners and managers of networks, as well as network service providers. Network here includes not only user-oriented websites, platforms, apps, mobile networks, e-commerce platforms and cloud platforms, but also information systems that support corporate services, such as communication facilities, industrial control systems, and office and business management systems. Arguably, any entity in China that uses computer systems connected to communications networks could be considered a Network Operator.	Cybersecurity Law of the PRC
Critical information infrastructure (CII)	Critical information infrastructure refers to information facilities that directly concern national security and stability and may seriously endanger national security and public interests in the case of data breaches, destruction or loss of functions, including but not limited to basic information networks that provide services such as public communications and broadcast transmissions, important information systems in the fields of energy, finance, transportation, education, scientific research, water conservancy, industrial manufacturing, healthcare, social security and public utilities, important information systems in State agencies and important internet application systems, etc. The specific scope of CII or the methodology to identify CII is not officially published yet.	Cybersecurity Law of the PRC; Critical Information Infrastructure Security Protection Regulation (Draft, 2017)

Appendix II: Chinese Law and Regulations for Cross-border Data Transfer

7 Nov, 2016 | Law

Standing Committee of the National People's Congress

Cybersecurity Law of the People's Republic of China

Establishing a fundamental framework for cyber security and data protection in China, the Law introduces the basic principle for the protection of personal information.

11 Apr, 2017 | Administrative regulation

Cyberspace Administration of China

Measures for the Security Assessment of Cross-border Transfer of Personal Information and Important Data (Draft)

The Measures introduce the principle of "informed consent" for the cross-border transfer of personal information, and set out measures for security assessment concerning cross-border transfers of personal information and important data.

27 May, 2017 | National standard

National Information Security Standardization Technical Committee

Information Security Technology - Guidelines for Security Assessment of Data Cross-border Transfer (Draft)

This Standard further clarifies the definition of a cross-border transfer of data and the scope of application for security assessment.

1 May, 2018 | National standard

National Information Security Standardization Technical Committee

Information Security Technology - Personal Information Security Specifications (GB/T 35273-2017)

The Specifications provide more detailed guidance for enterprises to improve their internal personal information protection system and practical operating rules. Since it became effective in May 2018, the Specifications have been widely adopted in the compliance practice of various sectors.

28 May, 2019 | Administrative regulation

Cyberspace Administration of China

Measures for Data Security Management (Draft)

The Measures give emphasis to the network operators' obligation in the safety administration of personal information and important data.

13 Jun, 2019 | Administrative regulation

Cyberspace Administration of China

Measures for Security Assessment of Cross-border Transfer of Personal Information (Draft)

The Measures replace the regulatory framework specified in the Measures for the Security Assessment of Cross-border Transfer of Personal Information and Important Data (Draft), and make clear the management principle under which personal information and important data are subject to separate supervision.

*CAC: Cyberspace Administration of China

** TC260: National Information Security Standardisation Technical Committee

Appendix III: Identifications of the MLPS

Level	Identifications
Level I	Ordinary networks whose destruction will cause damage to the legitimate rights and interests of relevant citizens, legal persons and other organisations, but will not cause harm to national security, social order and public interests.
Level II	Ordinary networks whose destruction will cause serious damage to the legitimate rights and interests of relevant citizens, legal persons and other organisations, or cause harm to social order and public interests, but will not cause harm to national security.
Level III	Critical networks whose destruction will cause particularly serious damage to the legitimate rights and interests of relevant citizens, legal persons and other organisations, cause serious harm to social order and public interests, or cause serious harm to national security.
Level IV	Particularly critical networks whose destruction will cause particularly serious harm to social order and public interests or cause serious harm to national security.
Level V	Extremely critical networks whose destruction will cause particularly serious harm to national security.

Appendix III: Obligations of Network Operators under the MLPS

Obligations	Identifications
General requirements for all networks/systems	1. Determine an individual responsible for the MLPS, establish a responsibility manage system for the MLPS, and implement the accountability system; 2. Develop systems for security management and technological protection, and set up systems with respect to personnel management, educational training, system security building, system security maintenance, etc.; 3. Formulate and implement procedures and workflows of security management of computer room, equipment and medium, etc.; 4. Prevent the infection and transmission of malware and guard against cyberattacks; 5. Adopt management and technical measures to monitor and record the cyber operating status, cybersecurity events, unlawful and criminal activities, and save, as required to do so, relevant cyber logs for the past six months or longer to be used to trace online violations and offenses; 6. Implement measures such as data classification, and back-up and encryption of Important Data; 7. Collect, use and process personal information according to the law, ensure the protection of Personal Information, and prevent Personal Information from being divulged, destroyed, falsified, stolen, lost or abused; 8. Implement measures designed to detect, block or eliminate illegal information, and adopt approaches to prevent illegal information from being spread to a wide extent and evidence for violations and offences from being destroyed or lost; 9. Fulfill duties with respect to network record-filing and identification of users' real names; 10. Report any events within 24 hours to the local public security organ with the jurisdiction; 11. Other cybersecurity protection obligations specified in laws and administrative regulations.

About the Author

- **LexisNexis & RELX Group**

  Maggie Yin (Director of Government Affairs at RELX Group)

  Flora Xu(LexisNexis China Head of Content)

  Julie Gao(LexisNexis China Practical Guidance Product Manager)

  Jennifer Wang(LexisNexis China Senior Legal Writer)

  Lucia Lu(LexisNexis Senior Marketing Executive)

  Anthony Barnard(LexisNexis Translation QA)

- **Zhong Lun Law Firm**

  Jihong Chen

  (Zhong Lun Partner)

  Sophia Han

  (Zhong Lun Senior Associate)

LexisNexis®

LexisNexis Legal & Professional is a leading global provider of regulatory and business information and analytics that help professional customers make better decisions, increase productivity and serve clients better. As a digital pioneer, the company was the first to bring legal information online with its Lexis® services. Today, LexisNexis Legal & Professional harnesses leading-edge technology and world-class content to help professionals work in faster, easier and more effective ways. Through close collaboration with its customers, the company ensures that organisations can leverage its solutions to reduce risk, improve productivity, increase profitability and grow their business. LexisNexis Legal & Professional, which serves customers in more than 175 countries with 10,000 employees worldwide, is part of RELX Group PLC, a world-leading provider of information solutions for professional customers across industries.

For more information, you may visit: www.lexisnexis.com.cn

中倫
ZHONG LUN

Zhong Lun Law Firm, founded in 1993, was one of the first private law partnerships to receive approval from the Ministry of Justice. After years of rapid development and steady growth, today Zhong Lun is one of the largest full-service law firms in China. With over 450 partners and over 3,000 professionals working in sixteen offices in Beijing, Shanghai, Shenzhen, Guangzhou, Wuhan, Chengdu, Chongqing, Qingdao, Hangzhou, Nanjing, Tokyo, Hong Kong, London, New York, Los Angeles and San Francisco, Zhong Lun is capable of providing clients with high-quality legal services in more than 70 countries across a wide range of industries and sectors through its specialised expertise and close teamwork. Zhong Lun's cybersecurity and data compliance team was the earliest professional team in China specialized in the field of cybersecurity and data protection. The partners of Zhong Lun have been invited to attend the legislative research and discussions of the Cybersecurity Law, the Regulations for the Protection of Critical Information Infrastructure Security (Exposure Draft), personal information protection rules and related national rules. In the field of technology, telecommunications and Internet law, Zhong Lun is highly recommended and ranked the 1st Class by Chambers and Partners, which is a reputable ranking institution worldwide. Several times, Zhong Lun has received key recommendations and awards from major legal medias such as Legal 500, Legal Band, Asia Law and Business, China Business Law Journal and other lawyer ranking agencies.

Acknowledgements

China-Britain Business Council

CBBC has been at the heart of the UK-China trade relationship for 65 years – it is a leading UK business network for China and enhances the independent voice of business within this relationship. It is a bilateral business network with longstanding and deep relationships and access to both the UK and China Governments. As such, with its membership of over 800 organisations, CBBC helps UK companies develop and grow their business with China, and Chinese companies expand and invest in the UK. CBBC does this through 13 offices in China and representative offices across the UK which provide Advice, Insight and Influence and access to an unparalleled network of your peers, suppliers and competitors. Everything CBBC does is focused on supporting member success and providing a clear return on members' investment. www.cbbc.org

Disclaimer

Any content of this report is for recommended reading or reference only and is not intended to and does not constitute any legal advices or views of LexisNexis and Zhong Lun Law Firm, the drafters of this report. If you have any need for legal advice, please ask for official legal opinions. The employers of the authors of this report, the authors themselves, and the agents thereof undertake no liability and give no warranty in relation to any likely consequences arising from the use of any information in this report.

Copyright

For more information about this report, or if you have any comments and suggestions, please contact:

DIT China: Liu.Tingting@fco.gov.uk; Jonathan.Dove@fco.gov.uk.

LexisNexis: julie.gao@lexisnexis.com

Zhong Lun Law Firm: chenjihong@zhonglun.com

CBBC: Mark.Hedley@cbbc.org; Yu.Lin@cbbc.org.cn

BUSINESS
IS
GREAT
BRITAIN & NORTHERN IRELAND