CHINA'S DATA PROTECTION LAWS

AND WHAT THEY MEAN
FOR THE UK'S HIGHER EDUCATION SECTOR

Advice 建议 | Analysis 解析 | Access 渠道

China-Britain Business Council
英中贸易协会

Disclaimer

1. All reasonable efforts have been made to ensure the data, insights and opinions in this report are accurate as of December 2022. Readers should be aware though that market conditions are subject to change.
2. This report represents the understanding and opinions of CBBC and does not constitute any legal, financial or investment advice. Readers are encouraged to evaluate the content of this report and seek professional advice when necessary.
3. The China-Britain Business Council will not be liable for any losses or damages that may result from the use of the content of this report.
4. The China-Britain Business Council is not responsible for the content or accuracy of any third-party websites that this report contains links to.

Foreword

Andrew Seaton, Chief Executive
China-Britain Business Council

We are delighted to continue delivery of our Comprehensive Higher Education Strategy Service (CHESS) with this report on China's Data protection regime, and what it means for international education providers.

Education partnerships and relationships with China are of strategic importance to many UK higher education institutions. CHESS provides the external expertise, resources, and guidance to help them shape and implement a future-proofed China strategy in an increasingly complex policy context.

This is achieved through a range of reports, analysis and insight, and practical workshops. The programme's emphasis on the key discussion points and policies affecting exchanges and cooperation in education is relevant whether your institution already has an advanced China footprint with a dedicated team on the ground through CBBC's Launchpad or your own office; your focus is on partnerships driving marketing, student recruitment, and transnational education (TNE); or you are seeking to expand your China activities.

Drawing on perspectives from CBBC's Education Team in the UK and China, together with expert advice from professional institutions, Chinese partners, and CBBC's member organisations, CHESS enables you to interpret significant policy changes in the sector and manage an operating environment which may be affected by evolving social, economic, and political developments.

The development of China's data protection laws is relatively young. UK institutions may therefore be unfamiliar with what they entail and how to comply with them. Despite an initial lack of specificity in certain areas, China's implementation of the Cybersecurity Law in 2017 was a watershed in the country's efforts to build a new and robust data protection regime. It serves as a foundation for the subsequent implementation of the Personal Information Protection Law and the Data Security Law, both of which elaborate on a range of regulatory concepts introduced by the Cybersecurity Law.

For UK higher education institutions, these developments mean less ambiguity. But while areas of uncertainty have indeed been clarified, the regulations governing data security have become more intricate, and navigating them may still be a challenge. For this reason, this report envisages two scenarios that UK education institutions are likely to encounter during their China journey and gives practical advice on regulatory compliance when faced with each of them.

I hope you find this report useful as you work with or within China. If you have any questions about its content, please do not hesitate to reach out to us at CBBC.

December 2022

China-Britain Business Council 英中贸易协会

Table of contents

Acronyms

FULL NAME	ACRONYM
Cyberspace Administration of China	CAC
Critical Infrastructure Information Operators	CIIO
Cybersecurity Law	CSL
Data Security Law	DSL
General Data Protection Rules	GDPR
Multi-Level Protection Scheme	MLPS
Ministry of Industry and Information Technology	MIIT
Network Operators	NO
Personal Information Protection Law	PIPL
PIPL Data Protection Officer	PIPL DPO
Personal Information Handler	PIH
Wholly foreign-owned enterprise	WFOE

Glossary

Critical Infrastructure Information Operator: Defined under the CSL, it is an organisation or business in charge of information related to critical infrastructure, which includes infrastructure for communication, information services, power, traffic, water resources, finance, public services, and e-government services.

Network Operator: Defined under the CSL, it is an organisation or business that collects user data through the internet.

Personal Information Handler (PIH): Defined under the PIPL, it is any individual or organisation that handles personal information and determines the purpose and the means through which to do so.

PIPL Data Protection Officer (PIPL DPO): The PIPL does not give a name to this role, but it is defined under the PIPL as the person in charge of personal information protection. Known as the PIPL DPO in this report, it supervises the handling activities of an organisation and must be appointed if the amount of personal information handled surpasses a threshold set by the CAC. This threshold is defined as being the personal information of over 1 million people or the sensitive personal information of over 10,000 people, or if the organisation's main business is processing personal information and it employs more than 200 employees.

Representative: Also known as the Entrusted Party, it is a role defined under the PIPL that must be appointed if an organisation conducting information handling does not have an office in China. The role is responsible for handling matters related to the protection of personal information and ensuring that such activities comply with the law. The Representative may handle information on behalf of the PIH and is in charge of communications between the organisation and China's supervisory authorities.

Sensitive personal information: Under the PIPL, sensitive personal information is defined as personal information that may cause harm to the security or dignity of natural persons if disclosed or illegally used. It includes information on religious beliefs, specific identity (identifying information), medical records, biometric characteristics, financial accounts, individual location tracking, and any personal information about a minor under the age of fourteen.

Executive summary

UK higher education institutions regularly need to work with important data and process sensitive personal information, and though they will be familiar with the General Data Protection Regulation (GDPR), they may be less so with China's own data protection laws. If these institutions are to work in or with China, whether recruiting Chinese students or establishing research partnerships, they will need to know, understand, and comply with China's local regulations.

Divided into seven chapters, this report provides an overview of the most important data regulations, while also giving practical advice through two scenarios to UK higher education institutions regarding compliance with China's data security regime. The report begins by explaining the evolution of the development of China's data protection laws, starting with the introduction of the Cybersecurity Law in 2017 and ending with the release in 2022 of the latest guidance on cross-border data transfers. The chapter that follows then takes a closer look at the Cybersecurity Law in order to shed light on this foundational piece of legislation, noting the ground rules that it set for data protection and the outlining of an accountability system that requires all data-collecting organisations to set security management systems and operating rules.

The third chapter discusses China's Personal Information Protection Law, which is of particular relevance to higher education institutions not only due to it governing the use of the personal information of individuals residing in China but also due to its extraterritoriality clause that governs the use of Chinese citizens' information outside of Chinese borders. Having established the basics of the laws regarding the handling of personal information, the three chapters that follow go into further detail about China's Data Security Law, how the Cyberspace Administration of China classifies data, handling sensitive personal information, and conducting cross-border data transfers that comply with regulations.

The last chapter looks ahead to potential future domestic and international policy changes that could affect the development of China's data regulations, such as the implementation of the Social Credit System Development Law and moves to streamline cross-border data transfers. It notes that legal uncertainties and rules that may be incompatible with existing international laws have the potential to hamper progress in this area.

UK higher education institutions already working with or planning to work with China will find this report to contain insightful and practical advice. China's data protection laws may initially appear challenging, but taking the time to engage with them and ensure compliance can open the door to the opportunities of the China market.

Introduction

Over the last decade, laws governing the collection, storage, transfer, and usage of data have become a cornerstone of the regulatory environment in many markets, including in China. Indeed, with China as one of chief sources of data created worldwide, [1] such laws have been among the most high-profile passed in China in recent years, attracting attention and commentary from business, legal, and administrative communities alike, both inside and outside the country.

Data protection laws are applicable in a wide range of sectors, from e-commerce and the creative industries to life sciences and healthcare. They are of particular relevance to the education sector though, where those providing services rely upon the accurate and timely collection of various types of data to ensure the quality, suitability, and safety of their offerings. For higher education institutions from the UK, the European Union's General Data Protection Regulation (GDPR) is likely to be among the main points of familiarity in the field of data protection. And while an understanding of the GDPR is, by itself, not sufficient to effectively operate within the China market, it remains a useful starting point due to certain similarities between its goals and practices and those of China's own data protection laws. To succeed in China, though, generally depends upon a deeper comprehension of local requirements.

At the most fundamental level, there are three key laws covering data protection in mainland China: the Cybersecurity Law (CSL), the Personal Information Protection Law (PIPL), and the Data Security Law (DSL), all of which were passed in the years since 2017. Together, and alongside various other measures issued by the authorities, they lay out the demands on those handling different types of data. For higher education institutions, meeting these demands can involve, among others, an understanding of: the differences between Network Operators and Critical Infrastructure Information Operators; the importance of roles such as that of the Personal Information Handler, as well as how these roles can fit into existing institutional infrastructures; and the classification framework that splits data into three categories.

More broadly, success in China is often best rooted in the knowledge that its data protection laws, while complex and at times fragmented, and while perhaps somewhat unfamiliar in comparison with the legal regimes in place in other markets, continue to be refined, deepened, and expanded upon. Crucially, there are solutions to the challenges that China's data protection laws present, and they are solutions that start with a thorough and up-to-date understanding of the history, development, and application of the laws themselves.

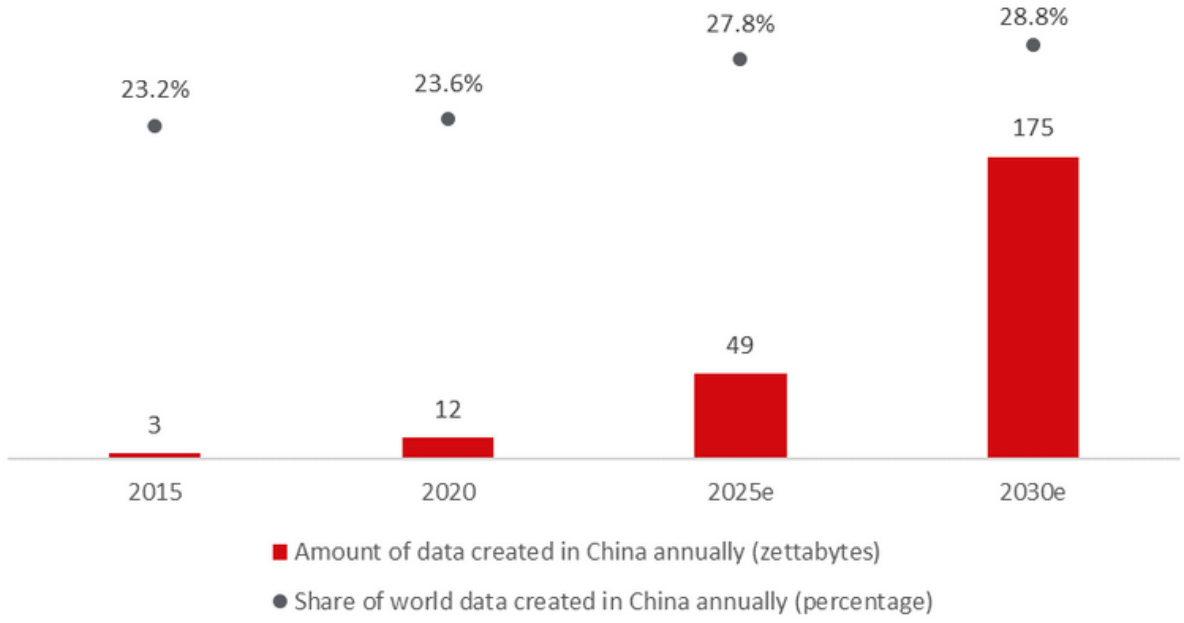
Looking ahead to 2023 and beyond, the China opportunity remains vast. More than ever for UK higher education institutions, it is one that they are well placed to grasp as the country continues to build and modernise its data protection infrastructure, and at the same time, they continue to refine and adapt their services alongside these changes.

Evolution of China's data protection regime

Data is integral to business and bureaucracy, and China's ambitious strategy to become a world leader in advanced technologies such as 5G, cloud computing, and AI will further elevate this trend. In step with its ambitions, a significant amount of total global data is created in China, and the quantity of data created in the country annually is growing at a faster rate than in any other country in the world. By 2025, data from China will account for 27.8% of the total global data created that year. [2] As China's digital footprint grows, policymakers around the globe are turning their attention to the question of how to secure and protect this data.

Figure 1

Quantity of data created in China annually and its share of total global data created annually, 2015-2030e (zettabytes and percentage) [3]



CSL

In China, the first major law regulating data was the Cybersecurity Law (CSL) in 2017, which, at the time, had a strong emphasis on national security. Since then, the focus has shifted towards data privacy and personal information. While this is partly due to the vagueness of the initial law — which included only superficial provisions regarding private data — growing consumer concerns over data theft and insufficient privacy protection have added pressure on Chinese policymakers to create a more coherent and comprehensive data protection regime.

The CSL created strong incentives for the Chinese government to establish clear standards for data collection and transfer. Thus, shortly after the CSL came into force, China published its first Personal Information Security Specification, [4] which defined personal data as including biometric information, personal addresses, and bank records. The specification was updated in 2020, adding further safeguards against an unauthorised collection of private data, for example by allowing users to opt out from specific online functions.

PIPL

Yet despite the regulatory activism sparked by the CSL in 2017, the legal foundations for individual data protection remained shaky and scattered across several laws. One particular problem was the lack of a uniform definition of the individual's right to his or her data, which was compounded by the fact that the exact nature of what constitutes a violation of privacy rules was stipulated in four different laws: the Criminal Law, the General Principles of Civil Law, the CSL, and the new Civil Code.

The passage of the Personal Information Protection Law (PIPL) [5] in August 2021 marked an important milestone as it provided for the first time a single, systematic framework for individual data protection. The many similarities between the European Union's (EU) General Data Protection Regulation (GDPR) and the PIPL have earned the latter the moniker 'China's GDPR', which, despite differences between the two, has brought China's data protection regime more in line with international standards.

More importantly, the PIPL has shifted the legal focus of China's data rules away from security and instead in a more consumer- and commercial-orientated direction. This shift has not only allowed for a more open and pragmatic discussion about the many challenges any new data regime faces in a continuously evolving technological environment, it has also raised the possibility for foreign organisations — such as UK higher education institutions — to participate more actively in future legislative processes; an input which was mostly ignored during the early stages of China's cyber-related rulemaking.

DSL

Nonetheless, national security remains important. The Data Security Law (DSL), [6] which came into effect in June 2021, is a strong reminder of this. The DSL affirms that the Chinese Administration for Cyberspace (CAC), a government agency, remains in charge of all data-related regulations. The law also highlights the importance of the two areas which particularly affect foreign institutions: how to manage sensitive personal information and how to conduct cross-border data transfers of such information.

Both above-mentioned issues are subject to evolving regulatory frameworks which have sprung up following the implementation of the CSL in 2017. Sensitive personal information — including biometrical, health, and financial data — is defined by the Personal Information Security Specification. [7] Data that falls into this category is subject to specific rules governing data storage, requirements in case of breaches and leaks, and data transfers.

Rules for cross-border data transfer have also been refined, as questions around data transfer across national borders are — almost by definition — a key concern of any cybersecurity regime. The first Draft Guidance on Data Cross-border Transmission Security Assessment came out shortly after the adoption of the CSL in 2017. Since then, this guidance has been updated four times with the latest version, the Measures for Security Assessment for Cross-border Data Transfers, [8] coming into effect in September 2022.

The following chapters will address in detail each of the three main laws — the CSL, the PIPL, and the DSL — as well as the regulatory frameworks for sensitive personal information and cross-border data transfers. Where relevant, scenarios dealing with key problems arising from these laws and regulations are included, providing guidance on how UK higher education institutions can deal with them.

Groundwork – the Cybersecurity Law

The CSL is the basis for all subsequent laws and regulations covering data collection, storage, and transfers. Understanding the background as well as the content of the CSL is therefore indispensable for understanding the Chinese government's thinking about data safety and data protection.

Originally, the CSL had a strong tilt towards national security and most of its early interpretation was seen in this light. The law's first draft was introduced in 2015, right after the passage of China's National Security Law, [9] and was, according to several analysts, [10] heavily influenced by the Edward Snowden affair in 2013, which had revealed the extent of US intelligence gathering in China and other countries.

The CSL's initial focus on national security and Article 28 of the CSL in particular — which requires all data-collecting entities in China to collaborate with Chinese law enforcement and security agencies — has also had a significant impact on public debate in other countries around Chinese multinational companies such as Huawei and ByteDance (the owner of TikTok). [11]

Nonetheless, the CSL has provided China with the groundwork of a data protection regime which, in its scope and depth, rivals that of the EU. The CSL is therefore not only useful for understanding Chinese data regulations but also for grasping global regulatory trends and developments more broadly.

Contact CBBC

Isabel Xu
Director Knowledge Economy, China
China-Britain Business Council, Shanghai
+86 (0) 21 3100 7900 Ext. 121
Isabel.Xu@cbbc.org

Thomas Clayburn
Senior Adviser, Knowledge Economy
China-Britain Business Council
+44 (0) 20 7802 2026
Thomas.Clayburn@cbbc.org

英中贸易协会

英中贸易协会

China-Britain
Business Council

ChinaBritain

China-Britain Business Council
Kings Buildings
Smith Square
London
SW1P 3HQ
+44 (0) 20 7802 2000

www.cbbc.org
enquiries@cbbc.org

Follow CBBC on WeChat