BCLP. Client Intelligent

**Insights**

# PART 5 OF 5: GAZING INTO THE FUTURE OF CHINA'S DATA PROTECTION LAW

Feb 20, 2022


## SUMMARY

China's data protection laws have been developing actively in the recent years. This article identifies some other Chinese legal instruments which are relevant to the protection of personal information, and discusses the current developments in China's data protection laws upon which businesses should keep an eye.


## INTRODUCTION

China's data protection law is not a single and unified piece of legislation. Rather, China's data protection regime comprises a multitude of legal instruments which, at present, is not practicable to be set out in an exhaustive list. One reason for this is that specific data protection rules and requirements may be found in Chinese statutes which govern primarily matters unrelated to data protection. Another reason is that China's data protection laws are relatively new (see timeline set out in Part 1 of this series), and many subsidiary legal instruments currently are being drafted and considered.

In this last part of the present series, we will complete our discussion on China's data protection law by setting out in brief a number of other Chinese laws identified by the Information Booklet published by the Hong Kong Privacy Commissioner for Personal Data ("PCPD") which are relevant, but which have not been mentioned already in other parts of this series. We also will provide a snapshot of what legal instruments currently are being drafted or developed.

## OTHER RELEVANT LAWS CURRENTLY OR SOON TO BE IN FORCE

There are numerous national and subsidiary laws which, to varying degrees, touch upon the protection of personal information (PI"). Depending on the business nature of the data handler, below are some examples of relevant laws which should be considered:

### 1. The Data Security Law ("DSL")

The DSL is a national law which came into force on 1 September 2021. It governs, very broadly, "any electronic or other form of record of information". It covers personal information, among many other kinds of information.

The DSL contains rules with regard to extra-territorial application, data handling, accountability of handler, security measures and cross-border transfers which are similar to what is set out under the Personal Information Protection Law ("PIPL"). The PIPL, being the legislation which specifically targets personal information, contains more detail than what is found in the DSL with regard to those requirements.

An important point to note regarding the DSL is that it provides for a tiered categorisation system for the protection of "important" data or information[1]. Handlers of "important" data are subject to additional data security controls. Note that the DSL does not further explain what constitutes "important" data and how such "importance" is determined. This likely is a matter which will be addressed in upcoming subsidiary legal instruments or announcements.

Where the personal information held by the data handler relates to national security or significant economic, livelihood or public interest issues, such personal information may qualify as "national core data" under the DSL which is subject to a more stringent regulatory framework[2].

## 2. Consumers' Rights Protection Law (2013 Revision)

The PIPL protects consumers by prohibiting differential treatment to consumers being implemented based on the data handler's analysis of personal information[3]. The 2013 Revision of the Consumers' Rights Protection Law also contains an array of provisions which protects personal information belonging to consumers.

For instance, consumers' personal information is to be respected during the purchase or use of goods, or when receiving services[4]. Business owners are required to protect the personal information of consumers in the following ways[5]:

- Obtain consumers' consent for the collection and use of personal information;
- Keep consumers' personal information strictly confidential; and
- Not to send commercial messages to consumers in the absence of consent.

Unreasonable and unfair restriction of consumers' rights or exclusions of liabilities by way of standard terms, notices, declarations or notices also are prohibited under this law[6].

The Chinese authorities have taken enforcement of this law seriously. In 2020, multiple major banks respectively were fined RMB 4 million to RMB 14 million, by way of administrative sanction[7], for breaches of consumers' rights pursuant to the Consumers' Rights Protection Law.

## 3. E-Commerce Law

China's E-Commerce Law came into force on 1 January 2019. It is closely linked with the Consumers' Rights Protection Law and the PIPL.

Specifically, e-commerce business owners are required to make clear to their users how to access, correct, delete their personal information and delete their accounts[8]. Personalised recommendations made to consumers based on preferences and spending records have to be presented to consumers together with non-personalised options[9]. Transaction histories are to be kept in record for not less than three years from the date of the completion of the transactions[10].

## 4. Announcements and guidelines issued by the Cyberspace Administration of China ("CAC") from time to time

With the increasing use of internet platforms and mobile application technologies, it may be anticipated that further regulation will ensue, which target data collection, processing and transmission which take place in cyberspace. Rules and guidelines that relate to PI protection already have been issued from time to time to cope with the fast-changing pace of digital trends..

Examples of recently issued rules and guidelines include the following:

**(a) Ways to Determine Whether a Mobile Application Collects Personal Information Illegally**"[11] announced on 28 November 2019.

This document sets out what constitutes (i) failure to make available to the public the rules for PI collection and use, (ii) failure to make clear the purpose, method and scope of PI collection and use, (iii) collection and use of PI without consent, (iv) collection of PI in breach of the necessity principle, (v) provision of PI to third parties without consent, and (vi) failure to provide channels or ways to delete or correct PI, or to lodge complaints.

**(b)** "**Rules to Govern the Ecology of Cyberspace Content**"[12] which came into force on 1 March 2020.

These rules deal with what kinds of cyberspace content are encouraged and what content is illegal. The rules contain requirements which apply to "internet content creators", "internet content platforms" and "internet content service users". Chapter Seven of these rules expressly sets out how failure to comply with these requirements may lead to criminal sanctions and civil liability.

**(c) "Internet Users Public Accounts Management Rules**"[13] which came into force on 22 February 2021.

These rules aims to regulate user accounts on website, mobile application or online platforms which publish content to the public. The rules specify various requirements for service

platforms and internet account hosts, some of which relate to the protection of personal information safety.

**(d) "Rules to Determine the Scope of Necessary for Personal Information Collected and Used by Mobile Applications**"[14] which came into force on 1 May 2021.

These rules contain a list of 39 kinds of relatively common mobile applications, and the categories of personal information that are considered necessary for the provision of their respective services.

**(e) "Cyberspace Algorithm-based Recommendations Management Rules**"[15] which will come into force on 1 March 2022.

These rules aim to regulate the provision of personalised recommendations generated by computer programmes or algorithms based on various forms of data synthesis. The requirements under these rules generally are in line with the spirit and requirements of §24 of the PIPL. In particular, consumers are to be given the option to turn off or opt out from algorithm-based recommendations. Also, algorithms must not be used to implement unreasonable differential treatment among consumers.

## 5. "Implementation Guidelines on Internet Security Standards" issued by the National Information Security Standardization Technical Committee.

The National Information Security Standardization Technical Committee plays an important role in shaping the practical rules surrounding the use of internet-related technologies. As of January 2022, ten Implementation Guidelines have been made available to the public on issues such as artificial intelligence, mobile applications and remote working[16].

## 6. Subsidiary laws related to the financial industry published from time to time.

The PCPD identified in the Information Booklet the following subsidiary laws and legal instruments which target to protect specifically personal financial information:

**(a) "Notice by the People's Bank of China regarding the Effective Protection of Personal Financial Information by Banking Institutions**"[17] which came into force on 5 January 2011.

The Notice provides, among other things, that data breaches which involve personal financial information are to be notified to branch authorities of the bank within seven working days. It also prohibits cross-border transfer of personal financial information, unless otherwise allowed by law.

**(b)** "**Implementation Measures issued by the People's Bank of China for the protection of the rights of financial consumers**"[18] which came into force on 1 November 2020.

These Implementation Measures govern how financial institutions are to protect the lawful rights of financial consumers in the provision of financial goods and services. The requirements generally

are consistent with the PIPL and the "Notice by the People's Bank of China regarding the effective protection of personal financial information by banking institutions" mentioned above.

Among other things, these measures provide that the handling of consumers' financial data must comply with the principles of legality, appropriateness and necessity, and must be expressly consented to by financial consumers.

**(c) "Personal Financial Information Protection Technical Specifications"**[19] also issued by the People's Bank of China, effective from February 2020.

The Specifications provide guidelines for financial institutions on the security measures recommended for the collection, transmission, storage, use, deletion and destruction of personal financial information. The PCPD commented in the Information Booklet that although these Specifications are not legally binding, violation of these Specifications still may be regarded by the Chinese authorities as breach of relevant laws.

## RECENT DRAFT LAWS FOR PUBLIC CONSULTATION

In addition to the legal instruments identified above, which already are in force, below are some examples of recent draft laws and instruments which have been released for public consultation (as of January 2022):

| **Date of release** | **Draft law[20]** |
|---|---|
| 8 January 2021 | Cyberspace Content Management Rules (Consultation Draft for Revision)[21] |
| 26 April 2021 | Temporary Rules for the Management of Personal Information Protection by Mobile Applications (Consultation Draft)[22] |
| 10 July 2021 | Internet Security Screening Rules (Consultation Draft for Revision)[23] |
| 29 October 2021 | Assessment Mechanism for Data Export Security (Consultation Draft)[24] |
| 14 November 2021 | Cyberspace Information Security Safety Management Rules (Consultation Draft)[25] |
| 5 January 2022 | Mobile Application Content Management Rules (Consultation Draft)[26] |
| 22 January 2022 | Cyberspace Content Deep Feature Synthesis Management Rules (Consultation Draft)[27] |

## CONCLUDING REMARKS

China's data protection regime has been developing rapidly. Numerous subsidiary laws have been drafted or are in the process of being drafted to address specific areas within the broad umbrella of personal information protection.

Judging from the most recent publications and releases of information briefly set out above, a lot of effort has been put in by the Chinese lawmakers in the development of PI protection laws related to the internet or digital platforms. New laws have been rolling out quite frequently to cope with the fast-changing pace and nature of the digital economy. Businesses are encouraged to keep a watchful eye on the release and development of new laws, and frequently if not continuously to review internal policies and practices to ensure proper compliance with the laws.

---

[1] §21 of the DSL.

[2] Ibid.

[3] §24 of the PIPL.

[4] §14 of the Consumers' Rights Protection Law.

[5] §29 of the Consumers' Rights Protection Law.

[6] §26 of the Consumers' Rights Protection Law.

[7] Administrative sanction decision nos. 寧銀罰字〔2020〕第2號；東銀罰字〔2020〕第1號；長銀罰 字〔2020〕第8號；吉市銀罰字〔2020〕第2號；德銀罰字〔2020〕第1號

[8] §24 of the E-Commerce Law.

[9] §18 of the E-Commerce Law.

[10] §31 of the E-Commercial Law.

[11] Available on the CAC's website only in the Chinese language, at http://www.cac.gov.cn/2019-12/27/c_1578986455686625.htm.

[12] Available on the CAC's website only in the Chinese language, at http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm.

[13] Available on the CAC's website only in the Chinese language, at http://www.cac.gov.cn/2021-01/22/c_1612887880656609.htm.

[14] Available on the CAC's website only in the Chinese language, at http://www.cac.gov.cn/2021-03/22/c_1617990997054277.htm.

[15] Available on the CAC's website only in the Chinese language, at http://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm.

[16] TC260-PG-20211A, TC260-PG-20205A, TC260-PG-20204A, TC260-PG-20203A, TC260-PG-20202A, TC260-PG-20201A, TC260-PG-20191A, TC260-PG-20183A, TC260-PG-20182A, and TC260-PG-20181A. See website of the National Information Security Standardization Technical Committee as updated from time to time at https://www.tc260.org.cn/front/cbw.html?start=0&length=4&type=3.

[17] Available only in the Chinese language at http://www.gov.cn/gongbao/content/2011/content_1918924.htm .

[18] 中国人民银行令〔2020〕第5号. Available only in the Chinese language at http://www.gov.cn/zhengce/zhengceku/2020-09/18/content_5544652.htm.

[19] No. JR/T 0171-2020.

[20] All draft laws are available only in the Chinese language. English translations of the names are for reference only.

[21] http://www.cac.gov.cn/2021-01/08/c_1611676476075132.htm

[22] http://www.cac.gov.cn/2021-04/26/c_1621018189707703.htm

[23] http://www.cac.gov.cn/2021-07/10/c_1627503724456684.htm

[24] http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm

[25] http://www.cac.gov.cn/2021-11/14/c_1638501991577898.htm

[26] http://www.cac.gov.cn/2022-01/05/c_1642983962594050.htm

[27] http://www.cac.gov.cn/2022-01/28/c_1644970458520968.htm

## RELATED CAPABILITIES

- Corporate
- Data Privacy & Security

## MEET THE TEAM

**Glenn Haley**

Hong Kong SAR

glenn.haley@bclplaw.com
+852 3143 8450

---