

Insights

PART 1 OF 5: A QUICK OVERVIEW OF THE KEY INSTRUMENTS FORMING PART OF CHINA'S DATA PROTECTION REGIME

Feb 16, 2022

SUMMARY

The Hong Kong Privacy Commissioner for Personal Data ("PCPD") recently published an information booklet on China's newly promulgated Personal Information Protection Law ("PIPL"). The booklet provides useful guidance to Hong Kong and overseas businesses by summarising several PRC laws and regulations which should be considered in conjunction with the PIPL.

INTRODUCTION

China's Personal Information Protection Law ("PIPL") took effect on 1 November 2021. The law is expected to have a significant impact on businesses which have or are planning to have some presence in China. To assist businesses in the understanding of and compliance with the regulatory regime governing the protection of personal data, Hong Kong's Privacy Commissioner for Personal Data ("PCPD") published an information booklet^[1] (the "Information Booklet") which sets out the key requirements under the PIPL and some related laws and regulations.

In addition to a very useful discussion of the background to and the key requirements of the PIPL, the 90-page Information Booklet also helpfully discusses a number of other relevant laws and case precedents which may assist in the proper understanding and interpretation of the PIPL requirements.

The Information Booklet is available only in the Chinese language. In this series of five blog posts, we aim to provide a summary or brief overview of the array of relevant laws, regulations and case precedents which provide supplementary information, with a view to helping businesses better grasp the relevant requirements under China's data protection regime.

This present article, being the first of the five articles in this series, will identify the legal instruments set out in the Information Booklet as key documents forming part of China's data protection regime. This Part 1 of the series will be followed by:

- Part 2: the PIPL requirements as supplemented by other relevant laws, regulations and instruments
- Part 3: the PIPL and the Personal Information Security Specification

- Part 4: penalties and liabilities
- Part 5: gazing into the future of China's data protection law

China's data protection law is wide and rapidly developing. These blog posts are intended to be a starting point for businesses to get a taste of the breadth of the materials relevant to China's data protection law, and acquire a better understanding of the spirit behind it.

A QUICK OVERVIEW OF THE KEY INSTRUMENTS FORMING PART OF CHINA'S DATA PROTECTION REGIME

In the Information Booklet, the PCPD has identified nine key and most representative instruments (in addition to the PIPL) which form part of China's personal data protection regime. These nine instruments and the PIPL are set out below in the order of the date they came into force:

(i) The Decision of the Standing Committee of the National People's Congress of China ("NPCSC") on the strengthening of internet information protection dated 28 December 2012 (the "NPCSC's Decision")

The NPCSC's Decision stated that digital information from which a citizen's identity is ascertainable and which relates to personal privacy is protected by the PRC. Obtaining, sale or provision of such information to third parties by illegal means are prohibited.

(ii) The Ninth Amendment to the Criminal Law

The Ninth Amendment to the PRC Criminal Law came into effect on 1 November 2015. It formally criminalised the invasion of personal information by prohibiting the obtaining, sale or provision of a citizen's personal information to third parties by illegal means.

(iii) Cybersecurity Law

The Cybersecurity Law ("CSL") took effect from 1 June 2017. It aims to protect security in the cyberspace by setting out regulations on cyberspace monitoring, operational security, information security and emergency measures.

Articles 40 to 45 of the CSL set the ways in which network operators are allowed to collect and use personal information.

(iv) Provisions on the Cyber Protection of Children's Personal Information

The Provisions on the Cyber Protection of Children's Personal Information were adopted by the Cyberspace Administration of China and came into force on 1 October 2019. This piece of legislation targets to protect the security of information relating to children below the age of 14.

Key provisions include the following:

- The creation and/or dissemination of content which invades the information security of children is prohibited.
- Network operators are required to devise rules and user agreements which specially protect the personal information security of children.
- Informed consent of the parents or legal guardians of children (whose personal information is to be handled) needs to be obtained.

(v) Information Security Technology – Personal Information Security Specification

The Personal Information Security Specification (“PISS”) was issued by the State Administration for Market Supervision of the PRC and the Standardization Administration of the PRC on 6 March 2020. The current version came into force on 1 October 2020.

The PISS contains detailed implementation guidelines, principles and measures which provide potentially useful guidance for many businesses. The PCPD’s view as expressed in the Information Booklet is that although the PISS is not a legally binding instrument, it is important reference material that enforcement agencies will look at when monitoring compliance with China’s data protection regime as a whole.

(vi) The Civil Code

The current Civil Code was adopted by the National People’s Congress of China on 28 May 2020 and took effect on 1 January 2021. Book Four of the Civil Code concerns “Personality Rights”. Article 990 provides examples of what is encompassed by personality rights. The “right to privacy” is one of those rights.

Chapter VI, Book Four of the Civil Code contains specific provisions on the right to privacy and the protection of personal information.

Individuals have the right to request judicial relief (for example, monetary damages and injunctive relief) for breaches of personality rights^[2].

(vii) The Law on the Protection of Minors (2020 Revision)

The Law on the Protection of Minors (2020 Revision) was adopted by the NPCSC on 17 October 2020 and came into force on 1 June 2021.

This latest revision of the Law on the Protection of Minors introduced the protection of a number of personal information rights of minors below the age of 14.

(viii) The Decision of the Supreme People’s Court regarding the applicable laws to civil cases involving the handling of personal information using face detection technology (the “SPC’s Decision”)

The SPC’s Decision took effect from 1 August 2021.

As its name suggests, this instrument applies only to civil disputes which involve the handling of personal information with the use of face detection technologies. The SPC's Decision confirmed that a person's facial information falls within the ambit of "biometric data", which data is subject to more stringent regulations.

(ix) Data Security Law

The Data Security Law ("DSL") was passed by the NPCSC on 19 June 2021 and came into force on 1 September 2021.

The DSL covers more than just personal data. It is high-level national law which regulates the handling of data generally, with the aim of protecting data security while fostering the development and use of data. Although it does not specifically regulate "personal" information, its provisions are consistent and compatible with the PIPL requirements.

(x) Personal Information Protection Law

The last but obviously not the least - the PIPL which was passed by the NPCSC on 20 August 2021 and came into force on 1 November 2021.

The PIPL is China's most comprehensive piece of legislation. It deals specifically with the protection of personal data or personal information ("PI"). The PIPL has attracted much attention in the international arena, including for its similarity with the EU's General Data Protection Regulation (GDPR), particularly in that (i) it purports to have extra-territorial effect and (ii) it comes with hefty financial penalties.

Understanding relevant provisions in the ten instruments set out above is key to ensuring compliance with China's latest legal requirements regarding PI protection.

In Parts 2 and 3 of this series, we will discuss the relevant requirements in some more detail.

[1] Available on the website of the PCPD at:

https://www.pcpd.org.hk/tc_chi/resources_centre/publications/books/files/pcpd_china_pipl_book2021.pdf

[2] §§995 to 997 of the Civil Code.

RELATED CAPABILITIES

- Data Privacy & Security
- Corporate

MEET THE TEAM



Glenn Haley

Hong Kong SAR

glenn.haley@bclplaw.com

[+852 3143 8450](tel:+85231438450)

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be "Attorney Advertising" under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP's principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.