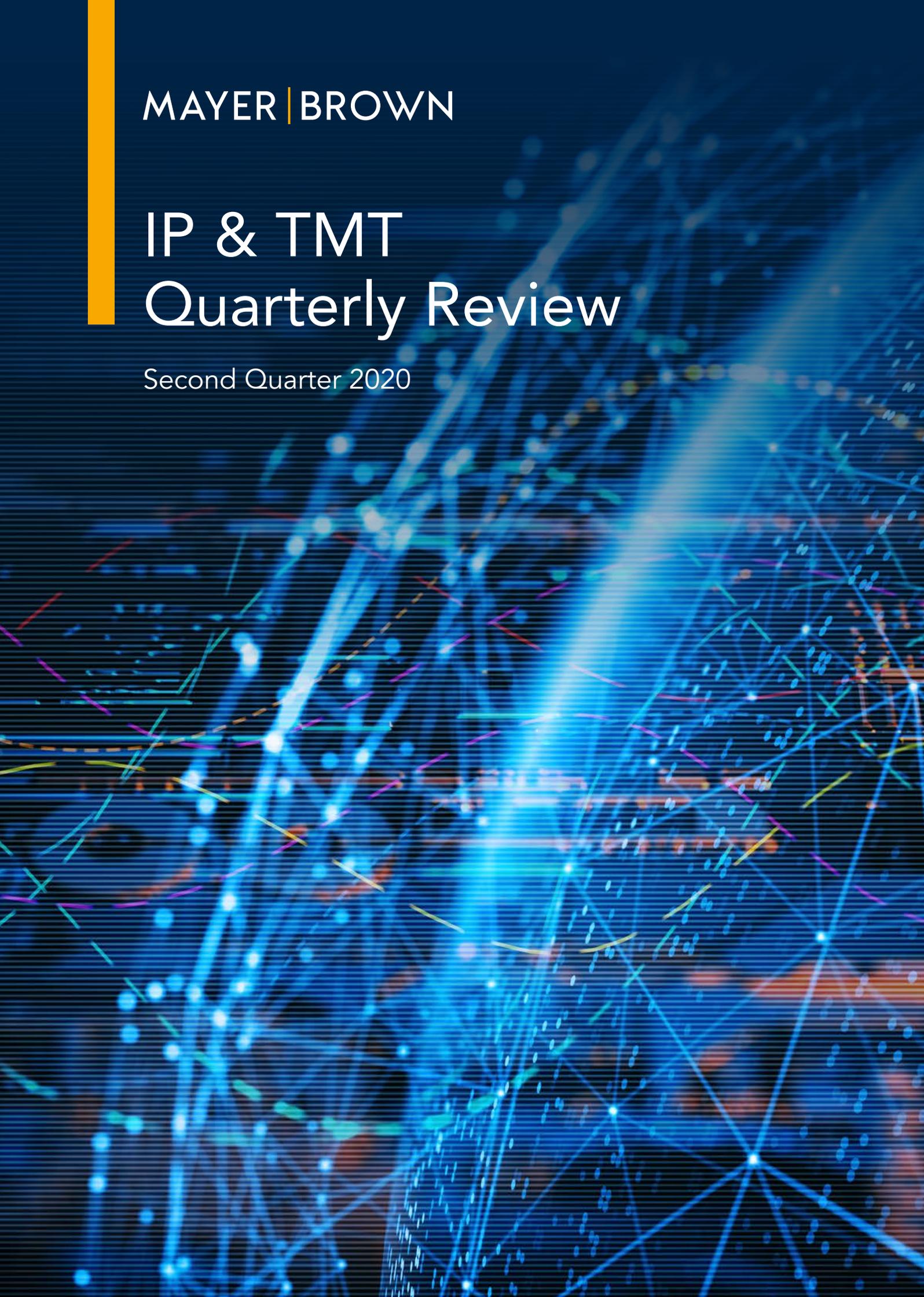




MAYER | BROWN

# IP & TMT Quarterly Review

Second Quarter 2020

The background of the page is a complex, abstract network graphic. It features a dense web of interconnected nodes and lines. The nodes are represented by small, glowing blue and white spheres, while the lines are thin, multi-colored strands in shades of blue, green, yellow, and red. The overall effect is a sense of dynamic connectivity and data flow, typical of a digital or network infrastructure visualization.

A night cityscape with digital network lines overlaid. The image shows a dense urban environment with numerous skyscrapers and buildings, illuminated by city lights. Overlaid on this scene is a complex network of glowing lines in various colors (blue, purple, pink, red) that connect different points across the city, suggesting a digital or data network. The lines are thin and have small circular nodes at their ends. The overall color palette is dark, dominated by the blues and purples of the night sky and the digital lines, with the warm yellow and white lights of the city buildings providing contrast. In the top left corner, there is a vertical yellow bar. The word 'Contents' is written in a large, white, sans-serif font, partially overlapping the yellow bar and the cityscape.

# Contents



2

## Intellectual Property

China

TURN BACK TIME: DOES TRANSFERRING THE DOMAIN NAME RESTART THE CNDRP LIMITATION PERIOD?

4

## Intellectual Property

Hong Kong

AT LAST! THE COPYRIGHT TRIBUNAL ISSUES ITS FIRST DECISION IN 22 YEARS

7

## Cybersecurity

China

SAFETY FIRST: CHINA'S NEW CYBERSECURITY REVIEW MEASURES

10

## Data Privacy

China

A STEP IN THE RIGHT DIRECTION: ENHANCED PROTECTION FOR PRIVACY AND PERSONAL INFORMATION IN THE PRC NEW CIVIL CODE

13

## Data Privacy

Hong Kong

REQUIREMENTS ON THE ELECTRONIC STORAGE OF DATA: RECENT SFC CIRCULAR

17

## Data Privacy

Singapore

PROPOSED AMENDMENTS TO THE PERSONAL DATA PROTECTION ACT – WHAT'S IN STORE

21

## Contact Us

CHINA

# Intellectual Property

---

## Turn Back Time: Does Transferring the Domain Name Restart the CNDRP Limitation Period?

By **Gabriela Kennedy, Partner**  
Mayer Brown, Hong Kong

**Karen H. F. Lee, Counsel**  
Mayer Brown, Hong Kong

---

In June 2019, the China Internet Network Information Center (“**CNNIC**”) extended the limitation period to file a .cn complaint under the cnDispute Resolution Policy (the “**CNDRP**”) from two to three years<sup>1</sup>. But does the transfer of the domain name to a new registrant restart the clock? The recent decision in 章节四公司 (CHAPTER 4 CORP.) v. 林建河 (HKIAC Case No. DCN-1900893)<sup>2</sup> (“**Supreme Case**”) has shed further light on this issue.

### Background

CHAPTER 4 CORP. (“**Complainant**”), which owns numerous “**SUPREME**” trademarks, filed a CNDRP complaint with the Hong Kong International Arbitration Centre (“**HKIAC**”), seeking the transfer of the domain name <supreme.com.cn> created in 2006. However, 林建河 (“**Respondent**”) acquired the domain name between July and September 2017 – eleven years after

- 
- 1 See our previous article: “The Gift of Time: New Limitation Period for Filing a CNDRP Complaint”: [https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2019/10/asi\\_ip\\_tmt\\_quarterlyreview\\_2019q3.pdf](https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2019/10/asi_ip_tmt_quarterlyreview_2019q3.pdf)
  - 2 [https://www.hkiac.org/sites/default/files/ck\\_file-browser/IP/cn/decision/DCN-1900893\\_Decision.pdf](https://www.hkiac.org/sites/default/files/ck_file-browser/IP/cn/decision/DCN-1900893_Decision.pdf)

the domain name was first created, and two years before the new limitation period under the CNDRP came into operation. The Panel therefore faced a dilemma: could the Complainant avail itself of the CNDRP in order to recover the domain name?

## Which Limitation Period Applies?

Under the previous version of the CNDRP, a complaint had to be filed within two years of registration of the disputed domain name. The June 2019 amendments to the CNDRP extended this limitation period to three years. The Complaint was filed in April 2019, before the amendments to the limitation period had come into effect. Therefore, the Panel held that the two year limitation period applied in relation to the Supreme Case.

## Does the Transfer of a Domain Name Amount to a New Registration?

If the transfer of a domain name to a new registrant does not amount to a new registration, then the limitation period in the Supreme Case would have expired, as the disputed domain name was first created in 2006. However, if the transfer of the domain name (in July to September 2017) *does* amount to a new registration, then the complaint (filed in April 2019) would fall within the limitation period, and would be eligible to be determined under the CNDRP.

The CNNIC were asked to provide a recommendation on whether the complaint filed in the Supreme Case was eligible to be determined under the CNDRP. The CNNIC recommended that complaints should not be accepted where the domain name was created (i.e. first registered) outside the limitation period, regardless of whether the domain name had been subsequently acquired or transferred. Even though article 51 of the CNDRP Rules allows the CNNIC to provide an interpretation of the rules, the CNNIC is not allowed to participate in any CNDRP proceedings in any manner whatsoever. The majority of the Panel decided that the CNNIC's "recommendation" did not amount to an interpretation and, as such, was not binding.

The Panel referred to previous decisions and the Guide to HKIAC Domain Name Dispute Resolution.

Section 6.1 of the Guide to HKIAC Domain Name Dispute Resolution and the cited decision of *Beijing Suning Shangpin Appliance Co. Ltd. v. Eryue* (ADNDRC Case No. HK-1500764) support the position that the transfer of a domain name amounts to a new registration. In the same way as good faith use of a domain name by a previous owner cannot be carried forward and attributed to a subsequent owner, the transfer of a domain name should amount to a new registration. The Panel therefore held that the limitation period should be calculated from the date of transfer of the domain name to the Respondent, and the deadline to file had not yet expired when the complaint was submitted.

The Panel's decision in the Supreme Case is consistent with the generally accepted position under the Uniform Domain Name Resolution Policy, and the position taken by the panellists in *Leister Brands AV v. Chen Qiuhe* (HKIAC Case No. DCN-1500641). The panel in that case based their decision on the fact that Article 9 of the CNDRP referred to both registration and acquisition of a domain name in relation to circumstances that amounted to bad faith, and so similarly the transfer of a domain name should constitute a new registration. They also noted that to find otherwise could indirectly encourage cybersquatting.

## Takeaways

Whilst previous decisions are not binding, it seems that panels will continue to adopt the stance that the transfer of a domain name to a new registrant will restart the limitation period. This position, plus the longer three year limitation period, gives brand owners additional time to tackle cyber squatters who register <.cn> domain names. However, proactive monitoring of domain names is crucial to prevent a brand owner from being time barred from utilising the CNDRP. If time barred, brand owners would have to turn to lengthy and costly court proceedings to recover a <.cn> domain name that incorporates their brand. In the long run, it may be more cost effective for brand owners operating in China to secure as many <.cn> domain names as possible to pre-empt potential cybersquatters.

The authors would like to thank **Samantha Cheung**, Intellectual Property Officer at Mayer Brown, for her assistance with research for this article.

HONG KONG

# Intellectual Property

---

## At Last! The Copyright Tribunal Issues Its First Decision in 22 Years

By **Amita Haylock, Partner**  
Mayer Brown, Hong Kong

**Jacqueline W. Y. Tsang, Associate**  
Mayer Brown, Hong Kong

---

The Hong Kong Copyright Tribunal ("**Tribunal**") was established in 1997 as an independent quasi-judicial body to determine disputes relating to copyright licensing and licensing schemes. It recently handed down its first decision in *Neway Music Limited v Hong Kong Karaoke Licensing Alliance Limited* CT 2/2010 ("**Neway decision**"). Neway Music Limited ("**Neway**") requested the Tribunal to determine the reasonableness of fees in respect of reproducing karaoke music videos ("**KMVs**") under a licensing scheme.

### The Facts

From July 2010 to June 2015, Neway entered into a licensing scheme ("**Scheme**") with Hong Kong Karaoke Licensing Alliance Limited ("**HKKLA**"). HKKLA is a licensing body authorised by Sony Music, Warner Music and Universal Music (collectively, "**Record Companies**") to negotiate and grant KMV licences to karaoke establishments in Hong Kong.

Under the Scheme, HKKLA granted licences to Neway for the reproduction of KMVs in its karaoke outlets.<sup>3</sup> Also under the Scheme,

---

<sup>3</sup> Copyright subsists in KMVs as they fall within the definition of "film" under section 7 of the Copyright Ordinance (Cap. 528). As the reproduction and playback of KMVs constitute an act of "copying" under section 23 of the Copyright Ordinance, karaoke operators need to obtain appropriate licences to lawfully reproduce KMVs.

KMVs are categorised into two types:

- i. "Back catalogue" - defined as any KMV which is not a "New Release"; and
- ii. "New Releases" - defined as KMVs which are commercially published by HKKLA at any time during a Scheme year; concert KMVs; or KMVs which have been expressly excluded.

The licence fees for the use of "back catalogue" KMVs are calculated by reference to the number of rooms installed with karaoke facilities, rather than the actual usage of KMVs. Below is a brief illustration of the licence fees in respect of "back catalogue" KMVs<sup>4</sup>:

Number of rooms	Per room per annum (HK\$)
1-10	14,760
11 to 15 16 to 20 21 to 25 [...]	<i>[bulk discount on a gradual sliding scale from 5.6% to 23.9% applied]</i>
95 to 100	
Over 100	11,160

The key issue for the Tribunal's determination was whether the licence fees under the Scheme in respect of the "back catalogue" KMVs were reasonable.

## The Neway Decision

### APPROACH

When determining whether a licensing scheme is reasonable, the Tribunal must take into account matters listed under section 167 of the CO, which include:

- i. the availability and the terms of comparable schemes;
- ii. the nature of the work concerned;
- iii. the relative bargaining power of the parties; and
- iv. the availability of information relevant to the scheme in question to the licensees, or prospective licensees.

The Tribunal should also ensure that there is no unreasonable discrimination between licensees or prospective licensees under the licensing schemes.

### HOW TO MAKE A REASONABLE VALUATION OF FEES

In assessing what is considered to be a reasonable level of fees, the Tribunal considered the following three approaches:

- i. **an economic benefits approach** – where part of the profits which the licensee is expected to receive from the use of the copyright work under licence is identified as a reasonable licence fee;
- ii. **a cost of substitution approach** – where the reasonable licence fee should be determined by reference to the cost of obtaining alternative intellectual property rights (in the present case, this would be the cost of obtaining licences from the Record Companies for reproduction licences or synchronisation licences and the cost of production of the KMVs by Neway); and
- iii. **a comparable approach** – where the reasonable licence fee is determined by comparison to other licensing schemes.

The Tribunal applied the comparable approach. The Tribunal then proceeded to review several historical KMV licensing schemes in Hong Kong but eventually decided that none of these schemes are suitable comparisons to the Scheme.<sup>5</sup>

The Tribunal found that the Scheme was reasonable and its terms did not require any variation. The Tribunal considered that the structure of the Scheme aligned with the principle that the more one uses a copyright work, the more licence fee a user should pay. It was decided that the Scheme gave due consideration to the fact that a larger karaoke outlet with more rooms would have more usage of the KMVs, and therefore would be charged increased licensing fees. Further the Scheme did not discriminate against smaller karaoke establishments by charging larger establishments disproportionately less amount of licence fees per room.

<sup>4</sup> See paragraphs 192 and 193 of the Decision. The calculation of licence fees was submitted by HKKLA and accepted by the Tribunal.

<sup>5</sup> Reasons for this include the fact that other licensing schemes were designed for independent karaoke outlets (not karaoke chains), and under another licensing scheme, a lump sum annual licence fee was charged instead of a scale fee.

The Tribunal made an order for payment of the licence fees by Neway to HKKLA for “back catalogue” K MVs for the five-year period during which the Scheme was in operation.

### THE TRIBUNAL’S POWERS UNDER SECTION 156(4) OF THE CO

Neway also applied to the Tribunal for an order under section 156(4) of the CO to protect Neway from any potential copyright infringement proceedings by the Record Companies in respect of the use of its K MVs (after the Scheme ceased operation in mid-2015).

While section 156(4) of the CO empowers the Tribunal to make an order which should be “*in force indefinitely or for such period as the Tribunal may determine*” when confirming or varying a licensing scheme, the Tribunal ruled that section 156(4) of the CO does not allow it to determine the life of a licensing scheme. In other words, the Tribunal cannot extend a licensing scheme after it has ceased operation, and therefore, Neway would still be exposed to potential copyright infringement proceedings in respect of its use of K MVs post expiration of the Scheme.

## Conclusion

As the Tribunal’s first ever substantive determination, the Neway decision sheds some light on the interpretation and application of some of the relevant provisions of the CO. Neway recently filed an appeal to the High Court. It seems the music will play on for a while yet.

The authors would like to thank **Cheryl Yip**, trainee solicitor at Mayer Brown, for her assistance with research for this article.



CHINA

# Cyber- security

---

## Safety First: China's New Cybersecurity Review Measures

By **Gabriela Kennedy, Partner**  
Mayer Brown, Hong Kong

**Karen H. F. Lee, Counsel**  
Mayer Brown, Hong Kong

---

On 27 April 2020, the Cyberspace Administration of China ("**CAC**") and 11 other government agencies jointly issued the Cybersecurity Review Measures ("**Measures**"), which require technology products and services procured by critical information infrastructure ("**CII**") operators to undergo a cybersecurity review, if they present a risk to national security. The Measures sit under China's Cybersecurity Law ("**CSL**"), and are one of a host of guidelines and measures that have been issued by the Chinese government to provide further clarity on the application of the CSL.

The Measures came into effect on 1 June 2020 and replaced the Measures for Examining the Security of Network Products and Services (Trial) issued in 2017.

### What do the Measures Require?

Under the Measures, any network products or services procured by a CII operator must be assessed by the CII operator to determine whether or not they "may" present a national security concern. If the answer is yes, then the CII operator must apply to the Cybersecurity Review Office ("**CRO**") for a cybersecurity review ("**Review**") to be conducted. These obligations apply regardless of whether the network products and services are provided by a domestic or foreign provider.

Separately, CII operators are also required to include provisions in their procurement contracts with network product or service suppliers, which:

- i. impose an obligation on the supplier to provide their cooperation with any Review;
- ii. prohibit the supplier from illegally collecting users' personal information;
- iii. prohibit the supplier from illegally controlling or manipulating any user's equipment; and
- iv. prohibit the supplier from suspending the provision of any products or necessary technical support, without any justifiable reason.

However, no procurement contract can be executed by the CII operator until the Review is completed and the transaction is cleared.

## What Network Services and Products are Covered?

Network services and products are broadly defined to include core network equipment, high-performance computers and servers, mass storage devices, large databases and application software, cybersecurity equipment, cloud computing services, and any other network products or services that may have a substantial impact on the security of CIIs.

## What Entities are Classified as a CII Operator?

The definition of a CII operator remains broad and unclear. CII operators include entities in key sectors such as finance, transportation, utilities (e.g. energy and water), government and communications, and any other industries that the Chinese authorities identify as having the potential to cause serious damage to national security, national economy and people's livelihood and public interests in the event they suffer a security breach leading to any destruction or loss of function or data. Additional sectors have also been identified by the Chinese authorities as falling into the CII category, including media, e-commerce, e-payment, search engines, emails, blogs, cloud computing, enterprise systems and big data. However, the definition of CIIs (and therefore the operators who will be subject to the stringent obligations imposed on CII operators) still remains fluid. It is expected that sector-specific

authorities will issue further guidance on which entities should be classified as a CII operator.

## Procedure and Time Frame

When applying for a Review, CII operators should submit the following documents: (i) a completed declaration form; (ii) an analysis on the potential impact on national security; (iii) any procurement documents, agreements, contracts or other documents to be entered into; and (iv) any other materials that may be required for the Review. Upon receiving the application, the CRO will consider whether a Review is required and notify the CII operator of its decision within 10 working days. Where a Review is deemed to be necessary, the CRO will proceed to conduct a preliminary review which must be completed within the initial period of 30 working days from the date of written notification to the CII operator. This initial period may be extended for a further 15 working days, depending on the complexity of the situation.

After the CRO completes its initial assessment, it will provide its report to the relevant government agencies and industry-specific regulators for their opinion. Who these government agencies or industry-specific regulators are remains to be determined, as they are not expressly identified in the Measures. Such government agencies and industry-specific regulators must submit their opinions to the CRO within 15 working days. Where there are differing opinions, the CRO may invoke a special review procedure requiring an in-depth analysis of the risks. This special procedure may take a further 45 working days.

## Assessment Criteria for the Review

According to the Measures, any Review conducted by the CRO should take into account the following key factors:

- i. the risk of illegal control over, interference of or destruction of CIIs and the risk of theft, disclosure or damage of critical data following the use of network products and services;
- ii. business continuity concerns in relation to any disruption in the supply of network products and services to CIIs;
- iii. the security, transparency, diversity of sources

and reliability of supply chains, and the risk of supply chain disruption due to political, diplomatic or trade factors;

- iv. the network product and service providers' compliance with Chinese laws, administrative regulations and department regulations; and
- v. any other factors that may threaten the safety of CII and/or national security.

If a CII operator or a network product or service provider believes that the outcome of a Review is unfair or fails to be impartial, or there has been a breach of confidentiality, then they may report the matter to the CRO or the relevant government department. However, it is unclear what further action will or can be taken by such entities.

## Potential Implications for CII Operators and Suppliers

### (I) BUSINESS CONCERNS

Foreign suppliers have expressed concern that the new Measures may adversely affect their competitiveness and ability to enter the Chinese market. From a national security perspective, foreign suppliers may be deemed to be of higher risk. CII operators may therefore favour the use of local suppliers to avoid any possible lengthy and cumbersome review if they use foreign suppliers, which may result in a delay in supply chain operations and increased business costs.

Multi-national companies operating in China who have negotiated supply chain agreements at a global level, may need to seek assurances from their supply chain regarding compliance with these Measures, or look at domestic options.

### (II) PROTECTION OF IP AND CONFIDENTIAL INFORMATION

To assist with the Review, the Measures also require CII operators to provide the CRO and relevant government authorities with certain documents and information relating to the CII operator, its supplier and the relevant network services and products. The information may include sensitive or confidential corporate information, such as code reviews, deep product specifications and trade secrets. In order to protect such sensitive information, the Measures specifically require all trade secrets and intellectual property rights disclosed in the course

of the Review to be strictly protected by the relevant government agencies and personnel involved. However, the concern still remains as to how strictly this obligation will be enforced.

## Penalties for Violation

Any CII operator who violates the Measures will be penalised in accordance with the CSL and ordered to cease using the relevant network products or services. In particular, a fine of up to ten times the value of the procured network product or service may be imposed on the infringing CII operator, and a separate fine of up to RMB 100,000 may be imposed on the relevant persons in charge.

## Takeaway

With the introduction of the Measures, CII operators procuring network products and services for use in China may have to re-examine their supply chain. They will need to expend upfront time and costs to carry out an initial assessment on the potential risks to national security. But how should this initial assessment be carried out? What factors should the CII operator take into account? Whilst the Measures touch on the procedure and factors to be considered in relation to the CRO's Review, limited guidance is provided to help CII operators carry out their initial assessment. At this point in time, CII operators may wish to err on the side of caution, until further guidance is provided by the relevant government authorities.

CII operators will need to predict their procurement needs well in advance, to allow for sufficient time to comply with the Measures.

*The authors would like to thank **Samantha Cheung**, Intellectual Property Officer at Mayer Brown, for her assistance with research for this article.*

CHINA

# Data Privacy



---

## A Step in the Right Direction: Enhanced Protection for Privacy and Personal Information in the PRC New Civil Code

By **Gabriela Kennedy, Partner**  
Mayer Brown, Hong Kong

**Cheng Hau Yeo, Associate**  
Mayer Brown, Singapore

---

### Introduction

After much anticipation, the Civil Code was passed by the PRC National People's Congress on 28 May 2020, and will come into force on 1 January 2021. An extensive piece of legislation, the Civil Code contains 1260 articles and a section on the "Right of Privacy and Personal Information Protection", which extends the current scope of protection of privacy and personal information.

### Privacy and Personal Information

The Civil Code sets out separate requirements pertaining to (i) the right of privacy and (ii) personal information protection in the PRC.

#### (I) RIGHT OF PRIVACY

The Civil Code provides that all natural persons enjoy the right of privacy, which is

defined as the private life, space, activities and information that one is unwilling to disclose to others. This is the first time that the right of privacy is defined in a statute in the PRC – although the existing General Provisions of Civil Law (implemented in 2017) cited the right of privacy, it did not provide a definition. The Civil Code stipulates that any “private information” contained in one’s “personal information” shall be protected by rules pertaining to the right of privacy, and if no such rules are applicable, the requirements relating to the protection of personal information shall apply, thus clarifying that, while the concepts of privacy and personal information may overlap, they are not equivalent.

The Civil Code prohibits any organisation or individual from engaging in the following privacy-intrusive activities:

- a. intruding into another’s private life through phone calls, text messages, instant messaging tools, emails and flyers;
- b. entering, photographing or spying on another’s private space, such as his home or hotel room;
- c. photographing, spying on, eavesdropping on or disclosing another’s private activities;
- d. photographing or peeping at another’s private body parts;
- e. processing another’s private information; and
- f. infringing the right of privacy through other means (a catch-all provision).

The above restrictions are subject to exemptions, such as the express consent of the affected individual, or “acts reasonably carried out in order to safeguard the public interest” (which appears to give considerable latitude for surveillance activities conducted by state authorities).

## (II) PERSONAL INFORMATION PROTECTION

In relation to the protection of personal information, the Civil Code imposes requirements which are largely akin to the existing rules under the CSL and its related guidelines and specifications. For instance, the Civil Code specifies that organisations or individuals may only process (i.e. collect, store, use, edit, transfer, provide or disclose) personal information when they have, *inter alia*, obtained the personal information subject’s consent and disclosed the purpose, method and scope of the processing of personal information. Also, as with

the CSL, the Civil Code provides that technical measures shall be taken to ensure the security of personal information, and imposes obligations to notify data subjects and relevant authorities of data breaches, and confers data subjects with rights of access, correction and deletion of personal information.

Notably, the Civil Code applies to any organisation or individual as long as they collect, store, use, edit, transfer, provide or disclose personal information. The requirements under the Civil Code apply equally to both personal information “controllers” and personal information “processors” (i.e. entities which process personal information on another’s behalf and not for their own purposes). The personal information protection requirements under the Civil Code are subject to exemptions, such as acts reasonably carried out in order to safeguard the public interest, or where the relevant personal information has been voluntarily disclosed to the public (unless the processing of such personal information is expressly refused by the data subject or harms his material interest).

## What’s New?

The Civil Code is a noteworthy addition to the PRC’s existing laws, regulations and guidelines concerning personal information protection. It is the first time that a separate “right of privacy” has been encapsulated into law.

In terms of personal information protection, the Civil Code in theory has a broader scope of application (covering any organisation or individual as long as they collect, store, use, edit, transfer, provide or disclose personal information) as opposed to the CSL which only applies to network operators and critical information infrastructure operators. The Civil Code captures organisations that adopt both analogue and digital processes while the CSL focuses on digital ones. Given the all-pervasive use of technology in China, the distinction remains academic. In addition, while existing laws and regulations mostly lay down criminal and administrative sanctions for violations of personal information protection requirements (e.g. fines, warnings, suspension of business), the Civil Code provides for civil liability for non-compliance, such as damages, orders for cessation of breaches of the law and public apologies. As privacy awareness has increased in the last couple

of years, the Civil Code will give consumers greater bargaining power when dealing with companies that collect their personal data.

Finally, the Civil Code also gives individuals the right to access their personal information in addition to the rights of correction and deletion which are already covered under the CSL. At present, the right of access is only provided under the Information Security Technology – Personal Information Security Specification GB-T 35273-2017 (the “**PI Specification**”), a non-binding best practices standard issued in 2018, but not the CSL.

## Uncertainties Still Remain?

Similar to the CSL, the Civil Code only sets out high-level and generic requirements relating to privacy and personal information protection. It is short on detail, and lacks nuanced distinctions and distillations similar to data protection laws in other jurisdictions, such as the General Data Protection Regulation (“**GDPR**”) in the EU. It also does not distinguish between sensitive and general personal information, set out different requirements for personal information “controllers” and “processors”, or stipulate rules on automated decision-making, cross-border data transfers and the retention of personal information. Although detailed rules relating to these issues are encapsulated in the PI Specification, the PI Specification is a non-binding standard which lacks the same statutory force as the Civil Code or the CSL. It is therefore uncertain how much weight PRC courts will give to the guidelines in the PI Specification when interpreting the requirements under the Civil Code.

That being said, PRC authorities have been signaling their intention of formulating a comprehensive personal information protection regime over the past few years, and have announced plans to introduce a new Personal Information Protection Law and Data Security Law later this year. While no further details of the proposed legislation have been disclosed so far, it is anticipated that they will consolidate and possibly refine the piecemeal laws, regulations and non-binding national and local guidelines in the PRC on personal information protection. Hopefully, this will give more clarity to the PRC’s personal information protection regime and bring it closer to international standards.

## Takeaways

For businesses operating in the PRC, the introduction of the Civil Code signals an increase of the cost of non-compliance with privacy obligations – they will have to take into account potential civil liability in addition to criminal and administrative penalties stipulated under present laws and regulations such as the CSL. Businesses should also bear in mind the new requirements in relation to the right of privacy under the Civil Code, which are separate from personal information protection obligations. Meanwhile, they should closely track the developments of the proposed Personal Information Protection Law and Data Security Law which are expected to be introduced later this year.

As far as private individuals are concerned, the Civil Code provides them with a clearer route to seek civil remedies from entities that collect their data for breaching privacy or personal information protection rules. Nonetheless, given the exemption provided for acts reasonably carried out in the public interest, it is unlikely that the Civil Code would curtail the ability of state bodies to conduct surveillance activities and process the personal information of citizens.

*The authors would like to thank **Christopher C. H. Ng**, trainee solicitor at Mayer Brown, and **Samantha Cheung**, Intellectual Property Officer at Mayer Brown, for their assistance with research for this article.*



HONG KONG

# Data Privacy



---

## Requirements on the Electronic Storage of Data: Recent SFC Circular

By **Gabriela Kennedy, Partner**  
Mayer Brown, Hong Kong

**Karen H. F. Lee, Counsel**  
Mayer Brown, Hong Kong

---

As businesses are busy adjusting and adapting to the “new normal” brought about by the COVID-19 pandemic, Hong Kong’s Securities and Futures Commission (“**SFC**”) extended the deadline for compliance with the SFC’s Circular to Licensed Corporations - Use of external electronic data storage (“**Circular**”) by six months, from 30 June 2020 to 31 December 2020.

This much welcomed grace period gives licensed corporations (“**LCs**”), electronic data storage providers (“**EDSPs**”) and other stakeholders, additional time to implement the necessary measures and controls prescribed by the Circular.

### Background

Under section 130 of the Securities and Futures Ordinance (“**SFO**”), LCs must obtain the SFC’s prior written approval for any premises that will be used to store records or documents, which the LC is required to retain under the SFO and the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, or which relate to the carrying out of the LCs regulated activities (“**Regulatory Records**”). Prior to the Circular (issued in October 2019), it was unclear how the LCs could comply with this consent requirement if they electronically stored their Regulatory Records on the cloud.

The Circular provided clarification on the LCs' obligations on the electronic storage of Regulatory Records through EDSPs. SFC broadly defined EDSPs to include providers of:

- i. public and private cloud services;
- ii. servers or data storage devices at conventional data centres;
- iii. other forms of virtual storage; and
- iv. technology services where information is generated as part of those services and stored by that provider (or another data storage provider), and which can then be retrieved by such provider.

## LCs that Solely Use EDSPs to Store Regulatory Records

Pursuant to the Circular, any LCs that *exclusively*<sup>6</sup> rely on EDSPs to store their Regulatory Records must:

- i. **Obtain SFC's prior written consent:** LCs must obtain the SFC's prior written consent for the data centre used by the EDSP to store the Regulatory Records, for the purposes of section 130 of the SFO. The SFC must be satisfied that the data centre is suitable for the purposes of keeping the Regulatory Records. The LC should only use an EDSP that is suitable and reliable, taking into account the EDSP's operational capabilities, technical expertise and financial soundness. The LC must also provide details to the SFC regarding the principal place of business and branch offices of the LC in Hong Kong, from which the Regulatory Records stored by the EDSP can be fully accessed (such physical premises must also be approved by the SFC under section 130).
- ii. **Designate two Managers-In-Charge ("MICs"):** LCs will need to designate two MICs in Hong Kong who have the knowledge, expertise and authority to access all Regulatory Records stored with an EDSP, and must ensure that the SFC has effective access to these Regulatory Records upon demand and without undue delay. The MICs are also responsible (amongst

other things) for ensuring that appropriate security measures are in place to prevent the Regulatory Records from being subject to unauthorised access, alteration or destruction.

- iii. **Ensure access to audit trail information:** LCs must ensure that they can provide detailed audit trail information regarding any access to Regulatory Records stored by an EDSP, including ensuring that any user can be uniquely identified.
- iv. **Ensure notification of transition arrangements:** Prior to any termination, expiration, novation or assignment of the service agreement with an EDSP, the LC must notify the SFC of their proposed transition arrangement at least 30 calendar days in advance.
- v. **Ensure access by SFC:** LCs should ensure all Regulatory Records kept exclusively with an EDSP can be fully accessed by the SFC on demand, without undue delay, from the LCs premises in Hong Kong, and can be reproduced in a legible form (such physical premises having been approved under section 130 of the SFO). To this effect, the LCs must also:
  - a. issue a notice to the EDSP ("**Notice**"), authorising the EDSP to provide to the SFC, the LCs' data stored with the EDSP, pursuant to the exercise of the SFC's statutory powers (without notifying the LC that it has been so required), which must be countersigned by the EDSP; and
  - b. obtain an undertaking signed by the EDSP, if the EDSP is a non-Hong Kong company<sup>7</sup>, in which the EDSP agrees to provide the LCs Regulatory Records to the SFC, and to assist the SFC where required in the exercise of the SFC's statutory powers (without notifying the LC that it has been so required) ("**Undertaking**").

When applying for section 130 approval of the EDSP's data centre, if the EDSP is a Hong Kong company<sup>8</sup>, then the LC must submit to the SFC a confirmation that the EDSP is a Hong Kong company and a copy of the Notice (countersigned by the EDSP). If the EDSP is a non-Hong Kong

6 That is, where the LC does not contemporaneously keep a full set of identical electronic or hard copy Regulatory Records at premises used by the LC in Hong Kong approved under section 130 of the SFO.

7 Defined in the Circular to mean a company incorporated in Hong Kong or a non-Hong Kong company registered under the Companies Ordinance (Cap 622), in each case with its personnel and data centre located in Hong Kong.

8 Ibid 7.

company, then the LC must submit to the SFC both a copy of the Notice and the Undertaking signed by the EDSP.

## General Requirements for All LCs That Use EDSPs (Whether Exclusively or Not)

Under the Circular, the SFC reminds all LCs of their obligations under the Management, Supervision and Internal Control Guidelines for Persons Licensed by or Registered with the Securities and Futures Commission issued back in April 2003, to put in place effective policies and procedures for the proper management of risks related to client data and information, and implement effective information management controls to detect and prevent the data from unauthorised access, amendment or deletion.

In particular, whether or not an EDSP is used exclusively or non-exclusively to store Regulatory Records, LCs must adopt the following precautionary measures:

- i. implement policies and procedures for proper risk management and information management controls;
- ii. conduct due diligence on the EDSP relating to its service delivery;
- iii. maintain an effective governance process for the use of software applications, and to protect the security, authenticity, integrity, reliability, confidentiality and timely availability of the data;
- iv. implement a comprehensive information security policy to prevent unauthorised disclosure or misuse of client data and information;
- v. implement controls to ensure information is only altered by authorised personnel for proper purposes;
- vi. put in place an exit strategy so that the contract with the EDSP can be terminated without causing material disruption to the LC's operations;
- vii. ensure binding agreement with the EDSP to define allocation of responsibilities; and
- viii. assess the extent of its dependence and risk of reliance on a single EDSP if that EDSP suffers a significant disruption.

## Extended Deadline

Where the data centre of the EDSP has already been approved by the SFC prior to 31 October 2019 (i.e. the date of issuance of the Circular), then the LC must, without undue delay, provide the SFC's Licensing Department with:

- i. the names of the two appointed MICs and a confirmation that all Regulatory Records are accessible at the LC's principal place of business on demand by the SFC; and
- ii. the required Confirmation, Notice and a confirmation that the other requirements in the Circular have been complied with by no later than 31 December 2020 (as extended from the original deadline of 30 June 2020).

For any other LCs who were already storing Regulatory Records exclusively with an EDSP, prior to 31 October 2019, but who had not yet obtained the SFC's approval – the LC must promptly notify the SFC's Licensing Department and apply for section 130 approval without undue delay.

## Tackling Compliance

Industry associations, such as the Asia Securities Industry and Financial Markets Association (**ASIFMA**), the Alternative Investment Management Association (**AIMA**) and Hong Kong Securities Association (**HKSA**), have noted certain practical challenges in implementing the Circular, and have been in talks with the SFC to discuss alternative arrangements to meet the requirements.

Under the Circular, the SFC requires LCs that exclusively store their Regulatory Records with EDSPs to provide a Notice and obtain from their overseas EDSPs an Undertaking "substantially" in the form of the templates appended to the Circular. The current template Notice and Undertaking require EDSPs to provide Regulatory Records and assistance as may be requested by the SFC, without notifying their LC clients that they have received any such request.

Industry bodies reflected that it is difficult in practice to obtain the required undertakings from EDSPs, given the extra costs and time EDSPs will have to incur in providing documentation and assistance on demand to the SFC. In transmitting data to the SFC, EDSPs may also encounter difficulties reconciling requirements under the Circular

with data privacy laws of other jurisdictions. Under the EU's GDPR, an EDSP is a "data processor" and an LC is a "data controller". A data processor is not allowed to provide data to third parties, such as the SFC, except on instructions from the data controller, unless required to do so under the laws of the European Union or Member States to which the data processor is subject.

## Conclusion

In light of the ongoing dialogue between industry associations and the SFC on the challenges they face in implementing the Circular and finding workarounds, LCs and other stakeholders should be on the lookout for any changes or further guidance (e.g. FAQs) to the regulatory regime. In the meantime, LCs should continue to regularly review their data retention and storage practices, and their arrangements with their EDSPs, to take stock of whether they are in compliance with the SFC's current set of expectations.

*The authors would like to thank **Cheryl Yip**, trainee solicitor at Mayer Brown, for her assistance with research for this article.*

SINGAPORE

# Data Privacy



---

## Proposed Amendments to the Personal Data Protection Act – What's in Store

By **Karen H. F. Lee, Counsel**  
Mayer Brown, Hong Kong

**Cheng Hau Yeo, Associate**  
Mayer Brown, Singapore

---

On 14 May 2020, the Ministry of Communications and Information and the Personal Data Protection Commission (“**PDPC**”) launched a public consultation on the draft Personal Data Protection (Amendment) Bill 2020 (“**Draft Bill**”). The Draft Bill proposes a suite of amendments to be made to the existing Personal Data Protection Act 2012 (No. 26 of 2012) (“**PDPA**”) and the Spam Control Act (Cap. 311A) (“**SCA**”).

### Key Proposed Amendments

The Draft Bill consolidates and refines the key amendments previously proposed by the PDPC in several public consultation exercises held between 2017 and 2019. The changes aim to enhance the accountability of organisations in relation to their collection, use or disclosure of personal data and increase public trust, as well as maintain the relevancy of the PDPA in light of recent technological advancements and an increasingly data-driven economy. The proposed amendments bring the PDPA more in line with regional and international data privacy standards. We have set out a summary of some of the key amendments below.

## (I) NEW CATEGORIES OF “PERSONAL DATA”

The Draft Bill introduces three new sub-categories of “personal data” under the PDPA:

- a. “Derived personal data” – this refers to personal data that is derived by an organisation in the course of business from other personal data about the individual or another individual in the possession or under the control of the organisation. However, this does not include data that is derived by the organisation using simple sorting or common mathematical functions, like averaging and summation.
- b. “User activity data” – this refers to personal data that is created in the course or as a result of the individual’s use of any product or service provided by the organisation. For example, transaction data or data collected by wearables and sensors.
- c. “User provided data” – this refers to personal data provided by an individual to the organisation.

As further discussed below, some of the proposed new obligations introduced under the Draft Bill may not apply to certain sub-categories of personal data. For example, “derived personal data” will not be subject to the data portability or data correction obligation. The intention is to protect and incentivise organisations to create innovative new products or services, which may be indirectly hindered by the data portability or data correction obligation if “derived personal data” were included. If an organisation were required to transfer any “derived personal data” to a competitor, then this could inadvertently result in the disclosure of confidential information that could damage the organisation’s competitive advantage.

## (II) MANDATORY BREACH NOTIFICATION

Currently under the PDPA, data controllers are not obligated to notify the PDPC or the affected data subjects in the event of any data breach. The new amendments would introduce a mandatory data breach notification requirement. In particular, data controllers would be required to:

- a. notify the PDPC where it determines that the data breach results in, or is likely to result in significant harm, or is of a significant scale, no later than 3 days after making such an assessment; and

- b. notify the affected individuals where it determines that the data breach results in, or is likely to result in significant harm to those individuals, as soon as practicable.

The PDPC is expected to issue subsidiary regulations to provide further details on these obligations, such as the definitions of “significant harm” and “significant scale”, and the method of notification required. According to the consultation document, a numerical threshold of 500 or more affected individuals will likely be prescribed for determining whether a data breach is of a “significant scale”.

Data intermediaries would also be required to notify the data controller without undue delay upon the discovery of a data breach. Certain exceptions have also been proposed in respect of these breach notification requirements. For example, where encryption or other technological protection measures have been implemented by the data controller, which minimises the potential harm that could arise from the data breach.

## (III) EXPANSION OF DEEMED CONSENT

The Draft Bill introduces two new sets of circumstances that may amount to “deemed consent” and can be relied upon in lieu of express consent. Specifically, “deemed consent” can be found where:

- a. the collection, use and disclosure of personal data is reasonably necessary for the conclusion or performance of a contract or transaction between an individual and an organisation; or
- b. the individual has been notified of the purpose of the intended collection, use or disclosure of his or her personal data, and has been provided with a reasonable period to opt-out but has failed to do so.

In order to be able to rely on (b) above, a data controller is required to conduct an impact assessment on the intended collection, use or disclosure of personal data, and implement measures to eliminate or reduce the risks of any adverse effects to the individual.

## (IV) NEW EXCEPTIONS TO CONSENT REQUIREMENT

The Draft Bill proposes two new exceptions to the consent requirement under the PDPA. These exceptions are:

- a. the “legitimate interests” exception – this allows the organisation to collect, use or disclose personal data without consent where such collection, use or disclosure is in the legitimate interests of the organisation, and the benefit to the public is greater than any adverse effect on the individual (e.g. for detecting or preventing illegal activities); and
- b. the “business improvement” exception – this allows the organisation to collect, use or disclose personal data without consent, for the following business improvement purposes: (A) operational efficiency and service improvements; (B) developing or enhancing products or services; and (C) knowing the organisation’s customers.
- c. the receiving organisations have a presence in Singapore (i.e. organisations that are either registered or have a place of business in Singapore).

Where the personal data to be ported contains personal data of other individuals (e.g. an individual’s social media account data may include names and photographs of third parties), the organisation does not have to obtain the relevant third parties’ consent when fulfilling a data porting request, provided that the data porting request is made in the requesting individual’s personal or domestic capacity.

If the Draft Bill is passed, the data portability obligations will likely only take effect at a later stage when additional regulations have been issued. These regulations are expected to contain further details on how to comply with the obligation, such as prescribing a “whitelist” of data categories to which the data portability obligation applies, imposing certain technical and process requirements in relation to the data porting, stipulating different data porting request models, and implementing additional safeguards for individuals such as establishing a “blacklist” of entities to whom porting organisations may legally refuse to port data.

The upcoming regulations will also provide for a list of exceptions to the data portability obligation which will likely be similar to the existing exceptions to the data access request obligation currently under the PDPA.

When relying on the “legitimate interest” exception, companies are required to conduct an impact assessment and implement measures to eliminate, reduce or mitigate any identified adverse effect to the individual, and determine that the benefit to the public outweighs any likely adverse effect to the individual. Companies are also required to disclose their reliance on this exception to the concerned individuals, for example, by making such disclosure in their privacy policy.

When relying on the “business improvement exception”, companies should also ensure that the personal data must not be used to make a decision that is likely to have an adverse effect on an individual.

## (V) RIGHT TO DATA PORTABILITY

Under the Draft Bill, individuals will be provided with a new right to data portability which will obligate data controllers, at the request of an individual, to transmit his or her personal data that is in the organisation’s possession or under its control, to another organisation in a commonly used machine-readable format.

However, data portability obligations will be subject to certain proposed limits. For example, these obligations will only apply if:

- a. the data porting request relates to “user provided data” and “user activity data” held in electronic form (accordingly, the obligation does not apply in respect of any request for porting of “derived personal data”);
- b. the requesting individuals have an existing, direct relationship with the organisation; and

## (VI) STRICTER ANTI-SPAM CONTROLS

The SCA, together with the PDPA, currently form the primary anti-spam legislation in Singapore. As it currently stands, the SCA only applies to unsolicited commercial messages sent to Singapore phone numbers in bulk (“**spam**”) but does not regulate such spam messages sent to instant messaging accounts over platforms such as Telegram or WeChat. Given the increasing popularity of such platforms (which are not based on the user’s telephone number), the Draft Bill introduces amendments to the SCA to expand its scope.

In addition, under the Draft Bill, the Do-Not-Call provisions under the PDPA will be amended to prohibit the sending of specified messages to telephone numbers obtained through the use of dictionary attacks and address harvesting software.

This amendment will align the Do-Not-Call provisions under the PDPA with the SCA, which currently prohibits the use of dictionary attacks and address harvesting software to generate electronic addresses for the sending of electronic messages.

#### (VII) INCREASED FINANCIAL PENALTIES

Amongst other proposals of enhanced enforcement powers of the PDPC, the Draft Bill will also increase the current maximum financial penalty for breach of the PDPA to: (a) S\$1 million; or (b) up to 10% of the organisation's annual gross turnover in Singapore, whichever is higher. This proposal will align the maximum penalties under the PDPA with those under the laws of the EU and Australia where a revenue-based maximum financial penalty is similarly adopted to serve as a stronger deterrent.

## Takeaways

The Draft Bill represents the first comprehensive review of the PDPA since its enactment in 2012. These proposed changes will help companies engaging in data-driven businesses overcome the challenges that they have been facing in complying with their obligations under a consent-focused data protection regime. Based on the responses received during the consultation exercise, public support for these amendments has been fairly high as organisations generally favour a shift towards a more flexible and risk-based approach.

On the other hand, increasing an organisation's accountability over the personal data under their control serves to boost public confidence and provide better protection of the individual's rights – an issue of increasing concern over the past few years in light of the numerous high profile data breaches, such as the SingHealth data breach in 2018 which has been called the "most serious breach of personal data" in Singapore's history.

The public consultation exercise ended on 28 May 2020 and the Draft Bill will now undergo final revisions before being introduced in the Singapore Parliament.



# Contact Us



**Gabriela Kennedy**

Partner

+852 2843 2380

[gabriela.kennedy@mayerbrown.com](mailto:gabriela.kennedy@mayerbrown.com)



**Amita Haylock**

Partner

+852 2843 2579

[amita.haylock@mayerbrown.com](mailto:amita.haylock@mayerbrown.com)



**Karen H. F. Lee**

Counsel

+852 2843 4452

[karen.hf.lee@mayerbrown.com](mailto:karen.hf.lee@mayerbrown.com)



**Cheng Hau Yeo**

Associate

+65 6327 0254

[chenghau.yeo@mayerbrown.com](mailto:chenghau.yeo@mayerbrown.com)



**Jacqueline W. Y. Tsang**

Associate

+852 2843 4554

[jacqueline.tsang@mayerbrown.com](mailto:jacqueline.tsang@mayerbrown.com)

---

Mayer Brown is a distinctively global law firm, uniquely positioned to advise the world's leading companies and financial institutions on their most complex deals and disputes. With extensive reach across four continents, we are the only integrated law firm in the world with approximately 200 lawyers in each of the world's three largest financial centers—New York, London and Hong Kong—the backbone of the global economy. We have deep experience in high-stakes litigation and complex transactions across industry sectors, including our signature strength, the global financial services industry. Our diverse teams of lawyers are recognized by our clients as strategic partners with deep commercial instincts and a commitment to creatively anticipating their needs and delivering excellence in everything we do. Our "one-firm" culture—seamless and integrated across all practices and regions—ensures that our clients receive the best of our knowledge and experience.

Please visit [mayerbrown.com](https://www.mayerbrown.com) for comprehensive contact information for all Mayer Brown offices.

This Mayer Brown publication provides information and comments on legal issues and developments of interest to our clients and friends. The foregoing is not a comprehensive treatment of the subject matter covered and is not intended to provide legal advice. Readers should seek legal advice before taking any action with respect to the matters discussed herein.

Mayer Brown is a global services provider comprising associated legal practices that are separate entities, including Mayer Brown LLP (Illinois, USA), Mayer Brown International LLP (England), Mayer Brown (a Hong Kong partnership) and Tauil & Chequer Advogados (a Brazilian law partnership) (collectively the "Mayer Brown Practices") and non-legal service providers, which provide consultancy services (the "Mayer Brown Consultancies"). The Mayer Brown Practices and Mayer Brown Consultancies are established in various jurisdictions and may be a legal person or a partnership. Details of the individual Mayer Brown Practices and Mayer Brown Consultancies can be found in the Legal Notices section of our website. "Mayer Brown" and the Mayer Brown logo are the trademarks of Mayer Brown.

© 2019 Mayer Brown. All rights reserved.

Attorney Advertising. Prior results do not guarantee a similar outcome.