Baker McKenzie Wong & Leow.

Intellectual Property
Singapore

Newsletter
July 2017

In This Issue:

Key Legal Developments in Singapore - Technology, Media, Telecommunications, Data Protection 2016-2017

Amendments to the Telecommunications Act

Introduction

The Telecommunications (Amendment) Bill was passed in Parliament on 10 November 2016 and took effect on 1 February 2017.

The amended Telecommunications Act provides a broad legal framework for the regulation of Singapore's telecoms sector, and provides the Info-communications Media Development Authority ("**IMDA**") with various powers to grant licenses, issue directions and codes of practices, and promulgate service standards.

These amendments were adopted with the purpose of ensuring Singapore remains relevant and effective in regulating and encouraging the development of the telecoms industry amidst rapid technological changes.

To ensure that the telecommunications sector is capable of meeting these demands, these amendments were adopted to further grant the IMDA the authority to facilitate the continued deployment of telecoms infrastructure.

Another objective of these amendments is to safeguard against anti-competitive behavior within the telecoms sector, such that consumers have full freedom to choose their preferred operator and services.

Proposed Amendments

The main amendments of the Telecommunications Act are as follows:

- The Telecommunications Act has been amended to clarify that parties who have control over the day to day management of a building must comply with the Code of Practice for Info-communication Facilities in Buildings. The IMDA will enforce the requirements on the legal owner of the building before reaching out to building managers like the Management Corporation or the Town Council.

- The IMDA is authorised to impose further regulations on 'springboarding'. This refers to mobile deployments sited at suitably high locations such as building rooftops to serve multiple buildings. Further consultations will be held with the relevant stakeholders.

- Telecommunication licensees must provide sufficient notice when entering buildings to deploy their infrastructure. Clear and accurate notifications must be issued to the building owner stating their intent and nature of the activities.

- Mandatory exclusive arrangements between Telecommunications service providers and building owners are prohibited. This will give end-users the freedom to choose their preferred operator and services. However, this will not prevent building owners from entering into promotional arrangements with operators. This will not apply to data centers, central offices and telecom exchanges.

- The IMDA is authorised to issue written notices and directions to licensees, developers, owners or occupiers of land or building to achieve compliance.

- The definition of "telecommunications service" has been amended to include the leasing of telecommunication cables.

(a) Establishment of an Alternative Dispute Resolution scheme for dispute resolution between telecommunication and media licensees and their subscribers.

- This will be mandatory for service providers, though consumers will have the flexibility to resolve their disputes through the ADR Scheme or through other avenues such as the Courts of Small Claims Tribunal.

- This will allow better management of consumer disputes, especially with regard to customer-specific contractual and billing issues.

- The IMDA will consult relevant stakeholders regarding the implementation of this scheme.

(b) Regulations regarding consolidations and corporate governance.

- The IMDA's directions with respect to consolidations can override the provisions of the Business Trusts Act, the Companies Act and the listing rules of a securities exchange.

- The IMDA is empowered to issue directions to enforce conditions of approval for mergers and acquisitions involving a designated telecommunications licensee, business trust or designated trust.

Implications

The Telecommunications sector should be aware of these amendments, especially in relation to the IMDA's position in the sector. Where possible, businesses in the telecommunications sector should participate in the upcoming consultations, including those involving the proposed framework for the alternative dispute resolution forum.

The Telecommunications Act will provide greater consumer protection vis-a-vis telecommunication service operators by establishing a new avenue of alternative dispute resolution for consumer-specific disputes with telecommunications operators.

Social Media Marketing Guidelines: Influencers

Guidelines on Interactive Marketing Communications & Social Media

On 29 August 2016, the Advertising Standards Authority of Singapore ("**ASAS**") issued its Guidelines on Interactive Marketing Communications & Social Media ("**Guidelines**"). The ASAS is the regulator of the advertising industry in Singapore and is comprised of representatives from key industry members, and is an Advisory Council to the Consumers Association of Singapore ("**CASE**"). It sets out best practices and industry standards for advertising in Singapore, including the Singapore Code of Advertising Practice.

The Guidelines were introduced in response to increased complaints about misleading advertising by influencers. According to public feedback, many consumers have been misled by the advertisements. In 2015, 91 complaints about online advertisements were received, as compared to 45 in 2014.

The Guidelines were developed in consultation with social media agencies, public agencies, corporations and members of the public, with the aim of establishing a standard of ethical conduct for advertisers on social media.

The key requirement of the new Guidelines is that marketing communication must be clearly distinguished from editorial or personal opinions. This is achieved by disclosing any commercial relationship or connection between the endorser and marketer of the product or service, where the connection may have a material effect on the weight or credibility of the endorsement. The onus of disclosure is on the marketer.

Crucial information that is likely to influence consumer decisions are to be disclosed within the marketing communication. This includes information such as prices, product characteristics and sale procedures and conditions.

Any digital marketing communication directed at children of a particular age group must be age-appropriate and suitable.

Implications

While the Guidelines are not legally binding, any marketers who breach them may face industry level sanctions. For instance, media owners may withhold advertising space or time from offenders. Alternatively, the ASAS may adopt "name and shame" measures against recalcitrant offenders. CASE may even take further action where an application has been made under the Consumer Protection Fair Trading Act.

For further information, please contact:

Andy Leck
Principal
+6564342525
Andy.Leck
@bakermckenzie.com

Lim Ren Jun
Principal
+6564342721
Ren.Jun.Lim
@bakermckenzie.com

Abe Sun
Local Principal
+6564342547
Vasan.Abe.Sun
@bakermckenzie.com

Personal Data Protection Commission: Advisory Guidelines on Enforcement of the Data Protection Provisions

Introduction

The Personal Data Protection Act 2012 ("**PDPA**") established a general data protection law in Singapore that regulates the collection, use and disclosure of individuals' personal data by organisations.

On 21 April 2016, the Personal Data Protection Commission ("**PDPC**") issued an additional set of advisory guidelines relating to the enforcement of the data protection obligations in the PDPA. While not legally binding, the guidelines complement the PDPC's existing set of published advisory guidelines, and deal with issues relating to the PDPC's enforcement of the PDPA.

Issues that are discussed in the Guidelines include how the PDPC will address, investigate, and resolve complaints of data protection breaches that it receives, the directions and penalties the PDPC can impose following the conclusion of an investigation, as well as the rights of review and appeal available to parties who are aggrieved by a decision of the PDPC.

Enforcement Framework

The PDPA empowers the PDPC to enforce the Data Protection Provisions by conducting investigations into reported non-compliance with the PDPA, reviewing an individual's request to an organization for disclosure or correction of personal data in the organisation's possession and to direct parties to opt for alternative dispute resolution mechanisms like mediation.

Key cases

In relation to enforcement of the PDPA, there have been numerous successful investigations and prosecutions.

One notable case involved K Box Entertainment Group Pte Ltd ("**K-Box**"). K Box faced complaints for breach of the PDPA as a result of its failure to develop an adequate secure and safe IT security system or appoint a Data Protection Officer to develop data protection policies, which resulted in the breach of personal data of its members via malware that was installed in its systems. A $50,000 financial penalty was imposed on K Box.

In a separate but related case, Finatech Holdings, which had been engaged to develop and manage a Content Management System for K Box, was also found to have failed to fix the weaknesses inherent in K Box's IT security system. Although Finatech Holdings was merely the data intermediary, the PDPC still imposed a financial penalty of $10,000.

In the Guidelines, the PDPC highlighted that a key aggravating factor in determining whether to take enforcement action against an infringer is the severity of the infringement.

Factors determining the severity of the infringement include: intentional, repeated breaches of the Data Protection Provisions, obstruction of investigations, failure to comply with previous warnings and the volume of sensitive personal data the organisation handles.

Comments

These cases highlight the importance for corporations to navigate the requirements of the PDPA lest they face adverse publicity and financial penalties - as organisations that fail to protect personal data can be fined up to $1 million per breach under the PDPA.

One way of ensuring compliance is to appoint a Data Protection Officer. Under the PDPA, this is mandatory. Despite this, however, only 40% of organisations surveyed have a Data Protection Officer based on the PDPC's survey of 1,513 organisations between March and June 2016.

Organisations' appointed data protection officers should ensure they are equipped with the necessary skills to scrutinize and implement the companies' data collection, use and disclosure policies. To acquire these skills (or upgrade their existing skills), data protection officers should consider participating in the local certification programme that was recently announced by the PDPC on 13 March 2017.

Launch of New Government bodies

Info-communications Media Development Authority

The Info-communications Media Development Authority ("**IMDA**") was formally established on 1 October 2016 as the designated regulator of both the infocomm and media sectors. It is the product of a merger between the Information Development Authority and the Media Development Authority in an effort to streamline the framework governing the infocomm and media industries.

This formation of the IMDA, a joint regulatory body of both the infocomm and media sectors is in recognition of the growing convergence between traditional telecommunications providers and the infocomm media sector.

The IMDA also incorporates the Personal Data Protection Commission ("**PDPC**"), and through the PDPC, will be responsible for promoting and regulating data protection in Singapore.

Government Technology Agency

The new Government Technology Agency ("**GovTech**") was created on 30 September 2016 with the aim of playing an operational role by incorporating technological changes in the public sector, through cooperation with the private sector. This reflects the Singapore government's focus to on adopting emerging technology such as robotics and artificial intelligence in the government sector.

GovTech will work closely with public agencies to develop and implement digital services, platforms and solutions in the public sector.

GovTech will also be the implementing agency for the new Smart Nation and Digital Government Office, a new body formed under the Prime Minister's office and created to strengthen the Singapore government's organisation ability to exploit opportunities offered by recent technological advances.

Budget 2017: Push for Small and Medium Enterprises to 'go digital'

Initiatives to build use of digital technology

During the Budget 2017, the Government announced the allocation of $80 million in funding for the newly introduced 'SMEs Go Digital' Programme. This is aimed at helping Small and Medium Enterprises ("**SMEs**") build its digital capability to seize opportunities for growth in the digital economy.

The SMEs Go Digital Programme will help SMEs in three main areas.

First, by supplying pre-approved technology solutions. SMEs will be able to access a supply of Infocommunication Media solutions that have been previously tested and preapproved by the Info-communications Media Development Authority ("**IMDA**"). These solutions include digital ordering and payment, supply chain optimization and resource and billing management. This would be enhanced by Industry Digital Plans that will be made available at the end of 2017.

Second, SMEs will be able to obtain in-person help at SME Centres This will be achieved by the launch of the SME Technology Hub in the third quarter of 2017, where SMEs can get advice on areas such as data analytics, data protection and cybersecurity. For SMEs intending to use new information and communication technology solutions, the SME Digital Tech Hub can also guide them on the appropriate solutions that would enable them to make full use of the available technology.

Training will also be provided. The SME Digital Tech Hub is slated to hold workshops and seminars, and the Cyber Security Agency of Singapore will aim to train cybersecurity professionals.

Third, support will be provided for companies developing emerging technology solutions. For instance, A*Star has spearheaded the Operation and Technology Road-mapping Programme, where it works with companies to create a customized technology strategy to bring their research and development projects to fruition and will expand its efforts to support 400 companies over the next four years. Similarly, under the Headstart programme, A*Star will partner SMEs to develop intellectual property and enjoy royalty free and exclusive licences for up to 36 months. This is complemented by the Technology Access Initiative where A*Star will provide access to specialized equipment to companies looking to use advanced machinery to develop and test its prototypes.

Implications

These initiatives and projects provide greater commercial opportunities to businesses involved in the digital sector, particularly in its research and development efforts.

SMEs which take full advantage of these initiatives will be able to enter into the digital technology sector or utilize digital technology in its day-to-day businesses to improve productivity. However, SMEs should obtain advice and be aware of the risks of the use of new digital technology or products, for instance, in relation to liability under the Personal Data Protection Act and the Computer Misuse and Cybersecurity Act.

Moreover, in the course of the development of new products or research, businesses should protect its intellectual property rights. This is of paramount importance where the technology or digital solutions were developed in collaboration with or with the assistance of an external body.

Changes to the Computer Misuse and Cyber Security Act

Introduction

The Computer Misuse and Cyber Security Act ("**CMCA**") was enacted in 1993 to regulate the unauthorized use of computers to access or modify data. Under the CMCA using a computer to secure unauthorised access to any program or data held in other computers in order to commit an offence is a penal offence.

Amendments

The amendments seek to expand the scope of the CMCA in order to tackle the increasing scale and transnational nature of online crimes.

The amendments criminalise acts enabled by cybersecurity attacks. The use of personal data obtained via an act in breach of the CMCA would be an offence. It would also be unlawful to use hacked credit card details, even if the act of hacking was committed by another.

Acts enabling cybercrime such as obtaining or dealing in tools which may be used to commit a CMCA offence such as malware and port scanners are also criminalised.

The amendments now allow for the extraterritorial application of CMCA offences. The CMCA presently penalizes criminal acts committed while overseas against a computer located overseas, if the act causes or creates significant risk of serious harm in Singapore. Serious harm is defined as injury, death or disruption to essential services.

Multiple unauthorized acts against a computer over a period of time may be now combined in a single charge, allowing for the application for enhanced penalties where the combined acts result in high aggregate damage.

Impact on businesses

Businesses must be aware of the possible consequences should products or methods used be found to facilitate any of the above mentioned offences.

This is especially so for small and medium enterprises ("**SMEs**"), which may lack the capability to conduct proper compliance measures or risk assessment. However, the IMDA will introduce a new SME Technology Hub to provide in-person advice on areas including cybersecurity to these SMEs.

Proposed Cybersecurity Bill

New Cybersecurity Bill

As part of the National Cyber Security Masterplan 2018 to make Singapore a Trusted and Robust Infocommunication Hub by 2018, a standalone Cybersecurity Bill will be tabled in Parliament in 2017. This is intended to complement the current Computer Misuse and Cybersecurity Act("**CMCA**"), which criminalises activities like the unauthorized use, access, interception and modification of computers, data and computer services.

Intended Changes

On 10 July 2017, the Ministry of Communications and Information and the Cyber Security Agency of Singapore issued a Public Consultation Paper on the Draft Cybersecurity Bill.

For a summary of the key sections of the draft Bill, see our earlier Client Alert (*"Singapore Releases Public Consultation Paper on Draft Cybersecurity Bill"*).

Broadly, the new Cybersecurity Act will institute standards for incident report, audits and risk assessments, as well as facilitate sharing of cybersecurity information. The participation of critical infrastructure operators in cybersecurity exercises will be mandatory.

The reporting obligation is not presently mandated under the CMCA unless the Minister for Home Affairs specifically requires a person to do so.

The Cybersecurity Agency, a body established to manage cyber security strategy, education and outreach, will be empowered to manage cyber incidents and raise the standards of cyber security providers.

Potential Impact

Businesses should position themselves to be ahead of the curve and adopt a cyber security system that will be able to detect risks early, mitigate these risks and respond robustly. Training for employees to deal with cyber security risks and threats will be of paramount importance.

Businesses should keep themselves apprised of the upcoming developments in the cyber laws and ensure that they take regular steps to comply with its requirements.

www.bakermckenzie.com

Baker McKenzie Wong & Leow
8 Marina Boulevard
#05-01 Marina Bay Financial Centre
Tower 1
Singapore 018981

Tel: +65 6338 1888
Fax: +65 6337 5100