

## E-COMMERCE LAW IN SINGAPORE

### General

#### 1. **How can the government's attitude and approach to internet issues best be described?**

The Singapore government has been proactive and inclusive in its encouragement and development of Internet communications and e-commerce, by its establishment of a supportive legal and technical infrastructure, investments in technology and awareness-building. Policy-wise, it adopts a balanced and light-touch approach to ensure that minimum standards are set for responsible use of the internet while giving maximum flexibility to industry players to operate, and favours industry self-regulation.

### Legislation

#### 2. **What legislation governs business on the internet?**

- The *Electronic Transactions Act (Chapter 88)* (ETA) is a facilitative piece of legislation that confirms the legal validity and admissibility of electronic records, electronic and digital signatures and electronic contracts. It also sets out the role of certification authorities who verify the identities of persons issuing digital signatures, the licensing requirements of which are fleshed out in the *Electronic Transactions (Certification Authority) Regulations*.
- The *Computer Misuse Act (Chapter 50A)* deals with the abuse of computer systems and criminalises unauthorised access, modification, interference and interception of computer systems.
- The *Spam Control Act 2007 (No. 21 of 2007)* was passed to control spam, requiring businesses to comply with stipulated conditions in the distribution of electronic messages.
- The *Telecommunications Act (Chapter 323)* addresses the licensing of telecommunications systems and services, while the *Code of Practice for Competition* in the *Provision of Telecommunication Services* stipulates the rules by which telecommunications system operators and service providers are to play, to ensure fair and efficient market conduct and competition among them.
- Broadcast content is regulated under the *Broadcasting Act (Chapter 28)*, pursuant to which the *Class Licence Scheme* was established. Internet content providers and Internet service providers deemed licensed under such scheme are required to observe the *Class Licence Conditions* and the *Internet Code of Practice*.

### Regulatory bodies

**3. Which regulatory bodies are responsible for the regulation of e-commerce and Internet access tariffs and charges?**

The *Info-communications Development Authority of Singapore* (IDA) is the licensing authority and regulator of info-communications systems operators and service providers in Singapore. IDA is empowered to regulate Internet access tariffs and charges in Singapore and has the mission of creating a conducive, innovative and competitive info-communications environment.

The *Media Development Authority of Singapore* is responsible for managing media content to protect core values and safeguard consumers' interests and for contributing to the development of Singapore into a vibrant global media city, creative economy and connected society.

### Jurisdiction

**4. What tests or rules are applied by the courts to determine the jurisdiction for internet-related transactions (or contentions) in cases where the defendant is resident or provides goods or services from outside the jurisdiction?**

Singapore courts have civil jurisdiction over disputes in proceedings where the defendant (wherever situated) submits to such jurisdiction. They also consider jurisdiction (including with respect to cross-border Internet-related transactions and disputes) based on connecting factors such as:

- whether the parties have agreed to a specified jurisdiction in their contract, which the Singapore courts will generally give effect to;
- the choice of law provision in the parties' agreement, if any;
- where the tort (if applicable) occurred, which would be considered *prima facie* the natural jurisdiction.

The Computer Misuse Act (See Question 2) also provides for extra territorial jurisdiction by extending the operation of the said Act to any offender outside Singapore of any nationality if the offender himself or any of its computer, program or data was in Singapore at the time of commission of the offence under the Act.

### Contracting on the Internet

**5. Is it possible to form and conclude contracts electronically? If so, how are contracts formed on the internet? Explain whether 'click wrap' contracts are enforceable, and if so, what requirements need to be met?**

The ETA (see Question 2) puts to rest any doubt that contracts may indeed be formed and concluded electronically. Unless otherwise expressly stated by the parties, the conventional laws regarding formation of contracts are equally applicable to online contracts. This was upheld by the Singapore courts in the case of *Chwee Kin Leong Ors v Digilandmall* [2004] 2 SLR 594.

The legal validity of click wrap contracts is not altogether certain as there is no legislation or case law in Singapore expressly addressing the same. However, going by the judicial approach adopted in the abovementioned case of *Chwee Kin Leong Ors v Digilandmall* [2004] 2 SLR 594, it is imagined that a click wrap contract would be upheld as long as the online user agrees to its terms (such as at the website in question or via email).

**6. Are there any particular laws that govern contracting on the internet? Do these distinguish between business-to-consumer and business-to-business contracts?**

The ETA, which facilitates contracting on the Internet, does not distinguish between business-to-consumer and business-to-business contracts.

**7. How does the law recognise or define digital or e-signatures?**

The ETA defines:

- an "electronic signature" as "any letters, characters, numbers or other symbols in digital form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record"; and
- a "digital signature" as "an electronic signature consisting of a transformation of an electronic record using an asymmetric cryptosystem and a hash function such that a person having the initial untransformed electronic record and the signer's public key can accurately determine - (a) whether the transformation was created using the private key that corresponds to the signer's public key; and (b) whether the initial electronic record has been altered since the transformation was made".

The ETA provides that an electronic record or electronic signature satisfies any rule of law requiring writing or signature, but this does not apply to any rule of law requiring writing or signature in relation to wills, negotiable instruments, trusts, immovable property or documents of title.

**8. Are there any data retention or software legacy requirements in relation to the formation of electronic contracts?**

There are no separate stipulations on data retention or software legacy requirements in relation to electronic contracts. Instead, the ETA expressly provides that where a rule of law requires certain documents, records or

information to be retained, such requirement will be met by the retention of electronic records subject to satisfaction of conditions relating to accessibility, format, identification of origin and consent of the concerned authorities requiring the retention.

## Security

### **9. What measures must be taken by companies or ISPs to guarantee the security of internet transactions?**

There is no statute which imposes mandatory measures to be taken with regard to security of Internet transactions in general, although industry specific guidelines exist such as the “Internet Banking Technology Risk Management Guidelines”, established by the Monetary Authority of Singapore, which stipulate risk management principles and security practices in relation to Internet banking that banks in Singapore are required to adopt.

Under the “TrustSg” programme established by the National Trust Council (NTC), an industry-led organisation supported by the government, businesses which comply with stipulated standards of security and privacy, are accredited as such, thereby providing assurance to those who transact with them (see Question 24).

### **10. As regards encrypted communications, can any authorities require private keys to be made available? Are certification authorities permitted? Are they regulated and are there any laws as to their liability?**

Digital signatures are recognised under the ETA on the basis of approved certification authorities (CAs) as trusted third parties, verifying the identities of persons who issue such digital signatures with specific private and public key pairs. CAs come under the regulatory purview of the Controller of CAs, being the Director-General (Telecommunications) of IDA and are licensed pursuant to the requirements of the *Electronic Transactions (Certification Authority) Regulations*, which they must comply with.

A CA having access to electronic records or other material by virtue of such role is obliged to maintain confidentiality of the same, contravention of which is an offence under the ETA.

Although there is no specific written law authorising any authority to require private keys to be made available, the Controller of CAs is entitled to have access to or inspect any computer system (and data contained therein) and associated apparatus or material that is reasonably believed to have been used in connection with an offence under the ETA.

The *Criminal Procedure Code (Chapter 68)* empowers the police to access any information, code or technology which has the capability of retransforming or unscrambling encrypted data into readable and comprehensible format or text for the purposes of investigating a “seizable” offence (i.e. an offence for which the police may ordinarily arrest without warrant).

### Domain names

- 11. What procedures are in place to regulate the licensing of domain names? Is it possible to register a country-specific domain name without being a resident in the country?**

Singapore Network Information Centre Private Limited (SGNIC) is the registration authority for country code top level (ccTLD) domain names in Singapore i.e. domain names ending with “.sg”. SGNIC has appointed a number of registrars for the registration of such domain names which are generally limited to persons or entities resident or registered in Singapore.

- 12. Do domain names confer any additional rights (for instance in relation to trademarks or passing off) beyond the rights that naturally vest in the domain name?**

No.

- 13. Will ownership of a trademark assist in challenging a ‘pirate’ registration of a similar domain name?**

Through the mechanism of the Singapore Domain Name Dispute Resolution Policy (SDRP) adopted by SGNIC, the owner of a trade mark may challenge the registration of a domain name by proving each of the following grounds:

- the domain name is identical or confusingly similar to the trade mark (and for this purpose, ownership of the trade mark will certainly be helpful);
- the registrant has no rights or legitimate interests in respect of the domain name; and
- the domain name has been registered and is being used in bad faith.

### Advertising

- 14. What rules govern advertising on the internet?**

There is no specific written law which regulates advertising on the Internet, although sector-specific legislation, codes of practice, guidelines and standards governing advertisements generally in Singapore, apply equally to advertisements on the Internet (see Question 15).

15. Are there any products or services that may not be advertised or types of content that are not permitted on the internet?

The *Internet Code of Practice* imposes on Internet content providers and Internet services providers the duty to use best efforts to ensure that "prohibited material" is not broadcast via the Internet to users in Singapore. "Prohibited material" is material that is objectionable on the grounds of public interest, public morality, public order, public security, national harmony, or is otherwise prohibited by applicable Singapore laws.

Sector-specific legislation such as the *Human Organ Transplant Act*, (Chapter 131A), *Smoking (Control of Advertisements and Sale of Tobacco) Act* (Chapter 309), *Consumer Protection (Trade Descriptions and Safety Requirements) Act* (Chapter 53), *Indecent Advertisements Act* (Chapter 135), *Medicines (Advertisement and Sale) Act* (Chapter 177), *Films Act* (Chapter 107), *Betting Act* (Chapter 21) and *Securities and Futures Act* (Chapter 289), ban, control, restrict or regulate the advertisement of specified products, services and content in Singapore.

Guidelines such as the *Singapore Code of Advertising Practice* self-imposed by the advertising industry, and the *Code of Advertising Practice for Banks Code* by the Association of Banks in Singapore seek to promote high ethical standards in advertising in Singapore against the background of applicable law and practice.

#### Financial services

- 16. Is the advertising or selling of financial services products to consumers or to businesses via the internet regulated, and if so by whom and how?**

Restrictions on advertising or selling financial services products are found in industry-specific but generally (and not only Internet) applicable enactments like the *Securities and Futures Act* (Chapter 289), *Banking Act* (Chapter 19) and *Financial Advisers Act* (Chapter 110).

#### Defamation

- 17. Are ISPs liable for content displayed on their sites?**

Under the ETA, ISPs are not subject to any civil or criminal liability under any rule of law in respect of third-party material in the form of electronic records to which he or she merely provides access, if such liability is founded on:

- the making, publication, dissemination or distribution of such material or any statement made in such material; or
- the infringement of any rights subsisting in or in relation to such material.

However, the above exclusion does not affect any contractual or statutory obligation of an ISP e.g. to deny access to "prohibited material" (see Question 15).

**18. Can an ISP shut down a web page containing defamatory material without court authorisation?**

To the extent that the defamatory material may be considered as "prohibited material" (see Question 15), the ISP may shut down the webpage containing such material on the basis of its obligation under the *Internet Code of Practice* to prevent broadcasting it.

An ISP is further stated to discharge its obligations under the *Internet Code of Practice* if it denies access to sites notified to it by the Media Development Authority as containing "prohibited material" (see Question 15).

Intellectual property

**19. Can a website owner link to third-party websites without permission?**

A website provider is generally regarded as being entitled to link to third-party websites without permission provided that it does not do so in a manner as to be misleading or to cause rights to be infringed.

**20. Can a website owner use third-party content on its website without permission from the third-party content provider?**

Use of any third party's content that is the subject of copyright or other intellectual property protection, without permission of the third party, whether on a website or otherwise, (and such use not being within stated exceptions such as fair dealing) would tantamount to infringement of such copyright or intellectual property.

**21. Can a website owner exploit the software used for a website by licensing the software to third parties?**

Where the website provider has not obtained specific authorisation from the owner of the software (which is the subject of copyright or other intellectual property protection) to license the software to third parties, it cannot do so, since this would tantamount to infringement of such copyright or intellectual property.

**22. Are any liabilities incurred by links to third-party websites?**

See Question 19. Also, network service providers are generally excluded from liability for their role in providing links to third-party websites subject to its meeting certain conditions reflective of its limited involvement, and without

prejudice to any of its contractual or regulatory duties in its provision of network services or facilities.

#### Data protection/privacy

#### **23. What legislation defines ‘personal data’ within the jurisdiction?**

There is currently no general data protection legislation in Singapore. Instead, the collection and use of personal data are regulated to a certain extent by the common law, a multitude of statutory provisions that address the issue according to subject matter, various self-regulatory industry codes and the co-regulatory Model Data Protection Code for the Private Sector (Code) (see Question 24).

Personal data is defined in the Code to mean:

“data, whether true or not, in an electronic form, which relate to a living person who can be identified —

- from those data; or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the organisation”

Such personal data may include an individual’s name, age, weight, height, national registration identity card number, medical records, income, purchases and spending habits, race, ethnic origin and colour, blood type, DNA code, fingerprints, marital status and religion, education, home address and phone number.

#### **24. Does a website owner have to register with any controlling body to process personal data? May a website provider sell personal data about website users to third parties?**

Outside of industry-specific regulation, there is currently no general duty on a website provider to register with any controlling body in order to process personal data as such.

The Code (see Question 23) established by the NTC (see Question 9), sets out the prescribed standards of general personal data protection in Singapore on a voluntary accreditation basis. Organisations wishing to be accredited with the “TrustSg” status for being fully compliant with, *inter alia*, prescribed standards of personal data protection, may do so by adopting the prescribed code of conduct which includes the provisions of the Code.

Whether it is permissible for a website provider to sell personal data about website users to third parties, depends on whether such website provider:

- has voluntarily subscribed to the provisions of the Code for purposes of being accredited as a “TrustSg” organisation; if so, it will be subject to the restriction under the Code to ensure that “personal data shall - not be used or



disclosed to a third party for purposes other than those for which it was collected, unless the individual consents to such use or disclosure or certain permitted exceptions apply”; or

- is otherwise prevented from doing so under any contractual restriction or other sector specific laws that regulate the subject matter in question e.g. customer information under the *Banking Act (Chapter 19)* or end-user service information under the *Code of Practice for Competition in the Provision of Telecommunication Services*.

The *Spam Control Act (No. 21 of 2007)* notably prohibits the sending of an electronic message to electronic addresses generated or obtained through the use of "address harvesting software" or "a dictionary attack", the latter being "the method by which the electronic address of a recipient is obtained using an automated means that generates possible electronic addresses by combining names, letters, numbers, punctuation marks or symbols into numerous permutations". Where such means are used to determine the electronic addresses (i.e. email addresses or mobile phone numbers) of website users and the website provider sells such information to a third party who sends electronic messages to them at such addresses, not only will the third party be in contravention of the *Spam Control Act*, but the website provider selling the information may also be liable for abetting or aiding or conspiring with the third party to effect the contravention.

- 25. If a website owner is intending to profile its customer base to target advertising on its website, is this regulated in your jurisdiction?**

See Question 24.

- 26. If an internet company’s server is located outside the jurisdiction, are any legal problems created when transferring and processing personal data?**

The Code (see Question 24) applies to any personal data which is processed or controlled by the organisation in question, regardless of whether the data is transferred out of Singapore.

If the personal data relates to the customers of a bank in Singapore and is to be disclosed to an outsource contractor to perform the bank's operational functions outside Singapore (such as where its server is located outside Singapore), such disclosure by the bank shall be subject to such conditions as imposed by the *Monetary Authority of Singapore*.

### Taxation

- 27. Is the sale of online products (for example software downloaded directly from a website) subject to taxation?**

The manner in which products are sold, whether online or otherwise, does not determine liability for income tax, which is charged on income derived from or accrued or received in Singapore. To the extent that payment for software is made by a person in Singapore to a non-resident person, such payment would be subject to withholding tax in Singapore.

A supplier who is registered for purposes of Goods and Services Tax (GST), is liable to pay GST on goods or services supplied by him in Singapore (see Question 29).

A person who imports goods is required to pay GST if the value of such goods exceeds S\$400. However, no GST is payable for digitised goods downloaded from outside Singapore, regardless of the value of such goods.

**28. What tax liabilities ensue from placing servers outside operators' home jurisdictions? Does the placing of servers within a jurisdiction by a company incorporated outside the jurisdiction expose that company to local taxes?**

The location of servers does not determine liability to taxation (see Question 27).

**29. When and where should companies register for VAT or other sales taxes? How are domestic internet sales taxed?**

A supplier which makes taxable supplies of goods or services in Singapore with an annual value exceeding or likely to exceed S\$1 million, is required to be registered with the Inland Revenue Authority of Singapore for GST and to pay GST on its taxable supplies. Domestic Internet sales by such supplier are included in these taxable supplies and subject to payment of GST at the current rate of 7% of the supply price.

**30. If an offshore company is used to supply goods over the internet, how will returns (goods returned in exchange for a refund) be treated for tax purposes? What transfer-pricing problems might arise from customers returning goods to an onshore retail outlet of an offshore company set up to supply the goods?**

An offshore company which supplies goods (not being downloaded digitised goods) of a value exceeding SGD400 to a customer in Singapore, will cause the customer to be liable to pay GST on such goods. This GST cannot be claimed back in the absence of over or erroneous payment, unless a specific order is made by the Minister for its repayment on the basis that all or substantially all the goods in question have been or are to be re-exported.

Singapore adopts the OCED arm's length principle approach to transfer pricing. Therefore if an offshore company transacts with its Singapore associated enterprise on non-arm's length terms such as to cause the Singapore enterprise to

be attributed with no or less profits than would otherwise have been the case, the Singapore enterprise may be chargeable to tax as if it were an agent of the offshore company.

### Gambling

**31. Is it permissible to operate an online betting or gaming business from the jurisdiction?**

Gambling and the promotion of gambling venues are prohibited in Singapore subject to very limited exceptions. Notably, the *Civil Law Act (Chapter 43)* provides that subject to the stated exceptions, "all contracts by way of gaming or wagering shall be null and void". Hence the conduct of gambling business in Singapore, online or otherwise, is not permissible other than within the limited and generally inapplicable exceptions.

As a matter of policy, online games such as online role-playing and massively multiplayer online role-playing video games are distinguished from gambling and the conduct of business relating to such online games and the hosting of such online games are encouraged in Singapore under the *Singapore Games Bazaar* initiative.

**32. Are residents permitted to use online casinos and betting websites? Is any regulatory consent or age, credit or other verification required?**

Although the conduct of gambling business is strictly controlled, Singapore laws do not provide for extra-territorial jurisdiction over offshore Internet gambling sites and casinos. The status of residents in Singapore gambling at such sites seems more uncertain, perhaps for practical and enforcement policy reasons and as illustrated by Singapore cases surrounding offshore gambling transactions. Whether or not it is a matter of law enforcers turning a blind eye to the existence of Singapore residents gambling at online casinos and betting websites, this situation does not lessen the prohibitions under the *Betting Act (Chapter 21)*, *Common Gaming Houses Act (Chapter 49)* and *Private Lotteries Act (Chapter 250)* which effectively prevent the physical premises within Singapore where the Internet gambling site is accessed from being used in a manner such that it becomes a common betting house or betting information centre or such as to cause a private lottery to be conducted without the requisite permit.

### Outsourcing

**33. What are the key legal and tax issues relevant in considering the provision of services on an outsourced basis?**

Typically, such issues relate to:

- ensuring continued compliance with the regulatory and other obligations of the customer whose data is being processed in the performance of the outsourced services e.g. with regard to confidentiality of such data;
- whether the customer's employees are to be transferred or will be terminated in consequence of the outsourced services; and
- in the case of a cross-border outsource transaction, the jurisdiction where the outsourced services will be performed, the entity which will perform and to which payment for the services is to be made e.g. withholding tax may be applicable to such payments; governing law and dispute resolution jurisdiction.

**34. What are the rights of employees who previously carried out services that have been outsourced? Is there any right to consultation or compensation, do the rules apply to all employees within the jurisdiction?**

There is no general right of employees to be consulted on a proposed outsourcing transaction. However, if the outsource transaction involves a transfer of all or part of the customer's undertaking to the outsourcing contractor, the *Employment Act (Chapter 91)* provides in such instance that:

- the employees so transferred would not be considered to have been terminated by the transferor and their employment would be continuous into employment with the transferee; and
- the employees would have to be notified of various details of the transfer as soon as reasonable before it takes place.

Otherwise, if a consequence of the outsourcing transaction is that employees are terminated, then such termination would have to be effected in accordance with contract terms (including payment of the appropriate compensation if applicable) subject to the minimum stipulations on termination under the *Employment Act (Chapter 91)* in relation to those employees who do not hold a managerial, executive or confidential position.

Online publishing

**35. When would a website provider be liable for mistakes in information which it provides online? Can it avoid that liability?**

In Singapore, the common law rules on misrepresentation and mistake apply equally to transactions online and otherwise. A website provider who posts inaccurate information online recklessly, may be liable for the tort of deceit or the tort of malicious falsehood where the requisite elements of such torts can be proved. To avoid such liability, it is prudent to expressly and sufficiently disclaim responsibility for the accuracy of information provided online to prevent reliance being placed on such information.

Further, where a contract is purportedly entered into based on an online:

- misrepresentation, such contract may be avoided and/or damages may ensue;  
or
- mistake of fact, such contract is ineffective.

**36. If a website provider includes databases on its site, can it stop other people from using or reproducing data from those databases?**

To the extent that a database is an original compilation, it would qualify for copyright protection as a literary work under the *Copyright Act (Chapter 63)* if the author of such work is a citizen or resident of, or the work is first published or published within 30 days of first publication in, Singapore or a country which is party to the Berne Convention or a member of the World Trade Organisation.

The website provider as owner of such copyright may stop others from using or reproducing the database compilation without his authorisation but may be challenged from doing so with respect to the data from such databases.

Updates and trends

***Are there any emerging trends or hot topics in e-Commerce regulation in the jurisdiction? Is there any pending legislation which is likely to have consequences for e-commerce and Internet-related business?***

The *Electronic Transactions Act (Chapter 88)*, is under review and amendments to it are expected with special reference to the provisions excluding the sufficiency of electronic records and signatures in relation to certain documents and transactions (cf. Question 7 above) and on ISP liability (cf. Question 17 above).

Singapore is seeking to build the next generation national info-communications infrastructure comprising complementary wired and wireless networks under its iN2015 Master Plan.

The Singapore Government has also launched a new S\$70 million Infocomm Security Masterplan 2 (MP2) for the public, private and people sectors to work even more closely together in an effort to combat emerging cyber threats over the next five years and to hone the competencies and resilience of these sectors against cyber threats, further contributing towards the iN2015 Master Plan vision of turning Singapore into an intelligent nation and a global city, powered by infocomm.