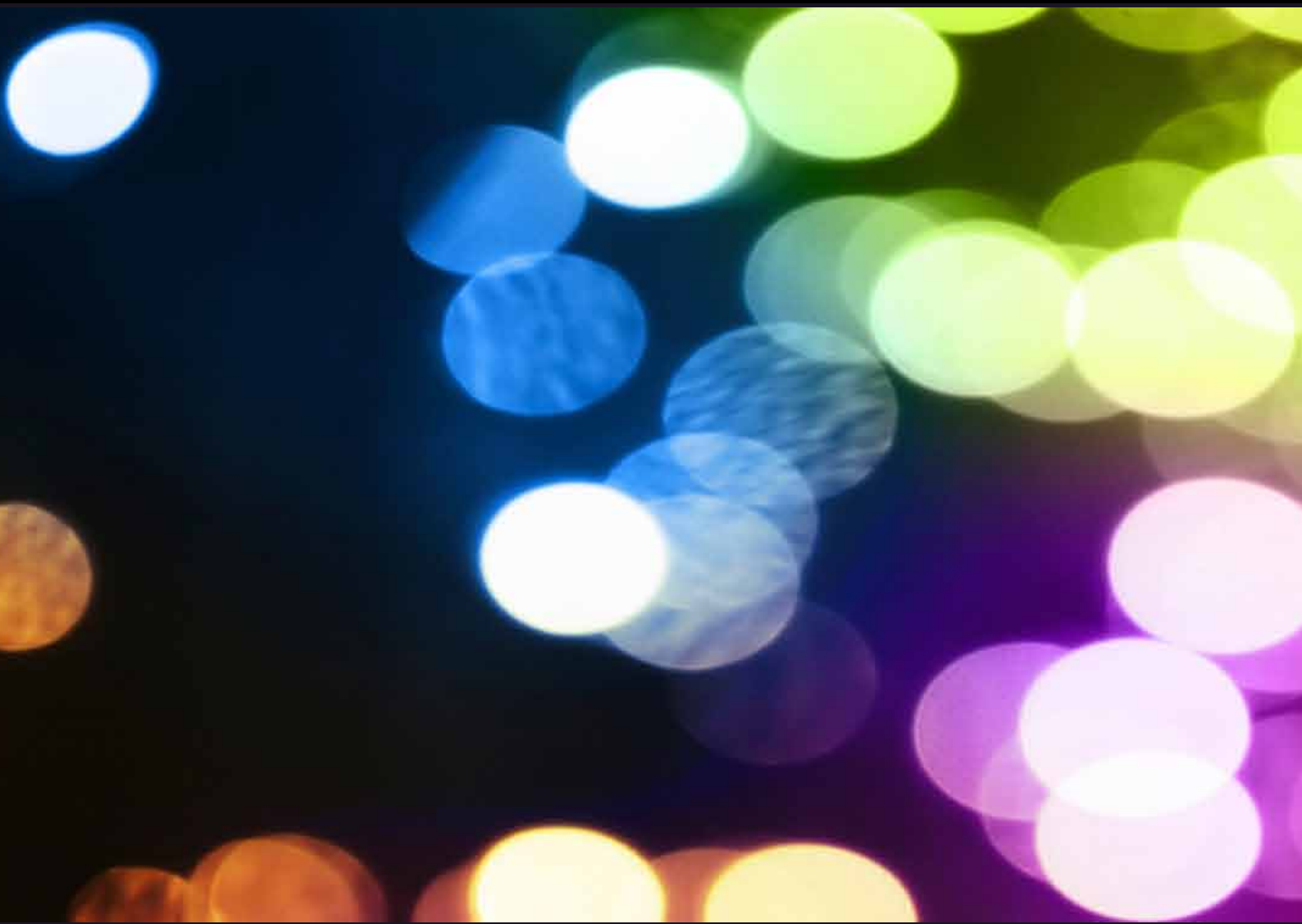
2012

New Singapore Data Protection Law

What you need to know

OLSWANG



New Singapore Data Protection Law

Singapore's first comprehensive data protection legislation was passed on 15 October 2012. This document sets out the key things you need to know about the Personal Data Protection Act 2012 ("Act") and what you need to do in order to get ready for compliance.

When does it come into force? When do I need to comply?

The bill was passed on Monday 15 October and is expected to come into force in January 2013 (a precise date has not yet been given).

For the general data protection provisions, organisations will have a grace period of 18 months to get ready for compliance however and so will not be subject to enforcement action until June/July 2014. There will be a grace period of 12 months until the Do Not Call Register provisions are enforced.

A European company is planning extensive expansion plans in South East Asia. It will physically set up offices in the next 24 months and will start a direct marketing campaign ahead of that to attract new customers including in Singapore. The company needs to factor in the new Act in thinking about its compliance obligations in the new territory and how this will impact its set up including the processes and policies it needs to put in place, its locations and IT architecture. It should start checking phone numbers against the Do Not Call Register from January 2014 regardless of whether or not it is physically sending the messages from Singapore at such time since it will be caught by the provisions if the recipient is present in Singapore when the message is accessed. However it is unclear how, in practice, the Act would be enforced against the company prior to it having a physical presence or place of business in Singapore.

What happens next?

The Act will come into effect. The new regulatory body will then be set up which will commence the task of preparing further regulation and guidance in relation to the Act and to educate the public and organisations about their rights and obligations.

Who needs to comply?

The Act applies to companies, associations and bodies as well as individuals who are resident in Singapore but not where they are acting as an employee or in a personal or domestic capacity. It does not apply to public bodies (which are subject to separate existing rules).

Unfortunately, the jurisdictional scope of the Act remains somewhat unclear at the current

time which will be unsatisfactory to many companies wanting to assess whether they will be caught by the Act or not. The current view is that it is unlikely that the Act will seek to have extra-territorial effect in respect of its general data protection provisions but will apply only to organisations that collect, use or disclose personal data in Singapore or transfer data out of Singapore. This would extend to foreign companies who have an office or place of business in Singapore but it is not clear that it would extend to a company based offshore who just happens to collect data from Singaporean customers along with other jurisdictions. This is a key issue that it is hoped will be cleared up in following regulations and guidance however.

In relation to the Do Not Call Register, the obligations only apply to senders of messages or calls to Singaporean numbers and where the sender is in Singapore when they send them or where the recipient accesses them in Singapore.

A couple set up a website to provide wedding guests with details and contact details of the venue and key members of the wedding party as well as posting pictures of the event itself and their guests. Since they are acting in a personal or domestic capacity, they will not be caught by the Act in relation to the processing of personal data that this will involve.

What type of data is caught by the Act?

The Act doesn't apply to every bit of data that an organisation may hold, only to "personal data". Personal data is data about an individual (whether or not it is true) who can be identified from that data or from that data and other information to which the organisation is likely to have access.

Obligations continue to apply to personal data for 10 years after an individual has died. Personal data that is more than 100 years old is not caught.

There are some carve outs in the Act for business contact details.

A company maintains a log of its employees' computer log on times. The company allocates each employee with a unique number and stores the log on times against these numbers rather than their names so that it is anonymous. It uses the information to get a better view of when staff are in the office so that it can manage resourcing levels better. Although the data in this database may itself be anonymous, if the company is able to 'unlock' the data by matching the unique number back to employees with other information that it holds, all such data could be deemed to be personal data and therefore caught by the Act.

What obligations does the Act impose?

In broad terms, the Act places obligations on how organisations collect, use and disclose personal data.

With nearly all of the obligations there is a “reasonableness” test applied so that an organisation must always think about what a “reasonable person would consider appropriate in the circumstances”. There is no further detail about how this test would be applied (not least since the courts themselves in Singapore have developed different interpretations in similar applications) and this is likely to generate some debate.

The main obligations are as follows:

Consent must be obtained from individuals before their personal data is collected, used or disclosed. Individuals must first have been given information about how their data will be processed so that they are giving consent on an informed basis.

Consent is not defined under the Act but it is hoped that guidance will emerge to confirm how this can be given. The Act does provide for certain exceptions and also that consent can be “deemed” if the individual gives the data voluntarily for a particular purpose and it is “reasonable” that the individual would have voluntarily given such data.

A European company is planning extensive expansion plans in South East Asia. It will physically set up offices in the next 24 months and will start a direct marketing campaign ahead of that to attract new customers including in Singapore. The company needs to factor in the new Act in thinking about its compliance obligations in the new territory and how this will impact its set up including the processes and policies it needs to put in place, its locations and IT architecture. It should start checking phone numbers against the Do Not Call Register from January 2014 regardless of whether or not it is physically sending the messages from Singapore at such time since it will be caught by the provisions if the recipient is present in Singapore when the message is accessed. However it is unclear how, in practice, the Act would be enforced against the company prior to it having a physical presence or place of business in Singapore.

Exceptions include emergencies threatening the life, health or security of the individual, national interest, artistic or literary purposes, certain news activities, business contact information, publicly available data and certain necessary disclosures in the context of business asset transactions.

In practice this will mean that organisations will need to develop privacy statements, notices and consent language to both inform consumers about their activities and to obtain the required consent.

The Act also provides that individuals must be allowed to withdraw their consent at any time.

A teenager has posted some pictures of himself at a party on a social networking site that have been reposted on other classmates’ pages. He is now worried that they might be seen by his teachers and could impact his chances of getting a place at university. It is possible that the teenager may be able to rely on the right to withdraw consent to the processing of the data by the site when he uploaded them in order to get the site to remove them from his page. It is more problematic in relation to the

classmates since they are likely to be deemed to be acting in a personal or domestic capacity and therefore not subject to the Act. He also will also be unable to stop teachers from accessing them where they are publicly available since the Act contains an exemption for such material.

Individuals must be given access to their personal data

With some exceptions, organisations must provide individuals with access to personal data they hold or control on request and information about how it is used. The Act does not provide that an organisation can charge for this nor does it prescribe time periods, the form the data must be given or other details. This can, in practice, be a tricky compliance area in other countries that have this obligation so it is likely to be another area where guidance will need to be developed.

Personal data must be accurate and requests for errors and omissions to be rectified adhered to

Organisations need to make a "reasonable effort" to ensure that data is accurate and complete where it is used to make a decision that affects an individual to whom the data relates or is likely to be disclosed to another organisation. Also, organisations must also respond to requests from individuals to correct errors or omissions in personal data held about them.

Personal data must be kept secure

There are no detailed security provisions in the Act nor specific obligations around notification of breaches as in some jurisdictions. The Act simply states that organisations must protect personal data in their possession or control by "making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks". Further guidance on what organisations need to do in order to meet this obligation will be particularly important.

Data must not be retained for longer than is reasonable for the purpose for which it was collected and no longer than is necessary for legal or business purposes

Organisations must not keep data indefinitely but must delete or anonymise their records when they are no longer needed for the purpose for which they were collected or where such retention is no longer necessary for legal or business purposes.

A company has engaged a headhunter to look for a new CEO and has been collecting various CVs and personal statements. The company should not continue to hold personal data relating to those individuals who do not go on to be appointed.

Take responsibility for data intermediaries

The Act does make a distinction between organisations primarily responsible for the collection and use of personal data on the one hand and data intermediaries which process personal data on behalf of those organisations on the other. Data intermediaries are subject to the data security requirements under the Act but in most cases the responsibility for compliance with the Act rests with the main organisation and they have to accept responsibility for all actions undertaken by intermediaries that they work with.

A food business uses a third party courier company to make home deliveries. It asks the courier company to get customers to answer a short questionnaire about the service which the food company then wants to use to provide bespoke food parcel suggestions next time the customer calls. The food business will not be able to blame the courier company for failure to obtain consent from customers to such use of their personal data. It is responsible for the actions of the courier company.

Compliance officers need to be appointed

Each organisation, regardless of size, needs to designate one or more person as responsible for ensuring the organisation complies with the Act whose details are made publicly available. Such appointment does not relieve the company of its responsibilities for compliance however and it does not appear that such officers will be held personally liable.

Restrictions on transfers of personal data out of Singapore

Organisations are not permitted to transfer personal data outside of Singapore unless they provide a "standard of protection to personal data so transferred that is comparable to the protection under this Act". At the moment the Act does not prescribe the detail of what this requirement will involve in practice and so we will need to wait for more regulations on this point. This is a big issue for international companies in particular and also for those using overseas data processing companies or servers and also a critical point for determining whether the Singaporean regime will itself be seen as "adequate" by Europe. It is not yet known whether the Singapore government will seek to go down the path of providing for approved contractual principles between transferor and transferee companies and/or whether it will draw up a list of approved countries/companies.

What is the Do Not Call Register and what will I need to do?

The Act provides for the establishment of a 'Do Not Call' register in Singapore that will allow subscribers to register their phone number and then organisations may not send a marketing or other promotional message to that number. It is expected that a time period for checking the register will later be implemented, therefore it is not the case that a company would need to check each and every time they make a call. In his speech, the Minister signalled the intention to prescribe a duration of 60 days for the first 6 months of the registry's operation and 30 days thereafter (which reflects the time period used in many other jurisdictions).

Even where a number is not registered, the Act also provides that marketing and promotional calls must identify the caller and organisation who has generated the message and provide information about how they can be contacted.

How will the Act be enforced? What penalties could be imposed?

A new Data Protection Commission is to be established which will be responsible for issuing guidance and advice, conducting research and studies and administering and enforcing the Act. It will also set up and run the Do Not Call Register.

This includes powers to review complaints, conduct investigations and inquiries and make directions including requiring an organisation it believes to be non-compliant to stop collecting, using or disclosing data or to destroy it. Directions can be enforced through the District Courts.

The Commission will also be able to impose fines and penalties as follows:

- Officers of body corporate may be personally liable
- Vicarious liability of employers
- Up to $10,000 for certain offences in relation to the Do Not Call Register
- Up to $1 million for failure to meet general data protection obligations
- Certain breaches may attract imprisonment for 12 months or even up to 3 years

The Act also provides for an appeal process.

There is also a private right of action via civil proceedings in the courts which could give rise to injunctions, damages or such other relief as the court deems fit.

What impact will it have on Singapore businesses?

For most companies in Singapore this law is big news and will involve time and cost in order to ensure that new procedures are in place to ensure compliance. Many international organisations operating in Singapore will already be familiar with navigating data protection regimes however and this change will simply mean that Singapore operations will need to be brought into the mix. In such case, it is important to note that the Singaporean data protection law is not just a “copycat” piece of legislation and it does contain some important differences from laws in other countries.

Over time, the rules may actually make business easier however as consumer confidence grows with the added protections provided and cross-border opportunities opened up where

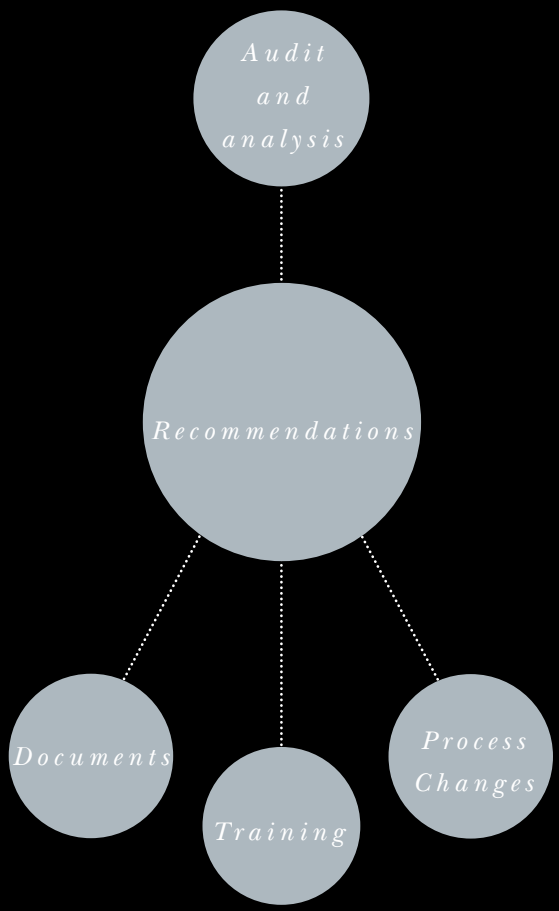
Singapore is recognised as providing adequate protections for companies wishing to transfer data to or through Singapore.

What do I need to do?

Whilst organisations are not expected to comply until the middle of 2014 in the main part and more regulations and guidance are expected, there will be work for all companies in Singapore to do to get ready for compliance.

Organisations are urged to seek advice now as to the key areas in which their business may be affected – particularly if they may be undertaking internal re-structuring, systems or procurement decisions over the next year or two where such issues should be taken into account now in order to avoid potentially costly moves.

An overview of suggested steps is below:



1. Audit and Gap Analysis

Conduct an internal review of personal data that is being processed by Singapore based operations or third parties that such operations contract and work with, how it is processed and where and to whom it is disclosed. For international organisations, or those already subject to sectoral data restrictions, look at any existing data protection processes and

policies that are already in place in order to identify whether there are any 'gaps' which need to be filled for Singapore.

Such an audit may take some time depending on the size and nature of the organisation and may involve interviews or other fact finding from different stakeholders, technical architecture.

Organisations might like to appoint their chosen data protection officer(s) at this point rather than later so that they can be involved in the development of the processes that they will then speak to and be responsible for.

2. Recommendations

Analyse the findings from the review and identify the processes and policies that need to be drawn up, any recommendations for technical or systems changes that might be needed.

3. Documents

Draw up and put in place the various documents and processes that have been identified as required. This may include:

Customers: privacy policy, terms and conditions, access process, correction process, opt-ins, marketing processes, etc

Employees: employment contract, employment handbook, consent, access, correction, etc

Suppliers (upstream and downstream): contractual provisions – may be flow through from existing legislative requirements, conduct diligence and additional audits where needed

Cross-stakeholder documents and processes: Information security policies and procedures, Counterparty diligence and contractual enforcement, cross-border data flow arrangements, data retention policy.

4. Training

Implement training for staff and other relevant persons around the organisation and also, where relevant, for subcontractors and other intermediaries engaged by the organisation in processing personal data.

5. Process Changes

Implement the new processes and procedures and keep them under review. Remember that any changes in the business may necessitate starting the cycle again – for example where new products or services are launched or there are changes in procurement or how data is used and processed.

Why is Singapore implementing this?

A consolidated data protection law offers many advantages for Singapore. For individuals, the change will bring protection in relation to privacy and use of personal information that other citizens in other countries around the world already enjoy including Hong Kong, Europe and Australia. As data becomes an ever more valuable commodity for businesses and the digital world means that it can be collected, used and disclosed on an ever increasing and instantaneous scale, individuals want to know that those that are behind such activity are subject to scrutiny and enforcement in how they conduct their activities.

From an economic perspective, data is big business and only getting bigger. In order to continue to compete on an international scale Singapore needs to be able to demonstrate that it is a good and safe place to do business in relation to data as much as it already does in other areas. International companies wanting to source suppliers or locate data centres need to know that the choice they make ensures that data will be held and processed securely and carefully. Another key aspect is that data often now tends to be transferred globally. By adopting a comprehensive but pragmatic data protection regime, Singapore hopes that organisations in regimes such as Europe that have restrictions on transfer to third countries are able to deem it as offering adequate protection.

How can I get more information?

Please contact:

Elle Todd
Partner

e elle.todd@oslwang.com
d +65 67208278

Please note that Olswang Asia is a foreign legal practice and is not licensed to advise on Singaporean law. This is an English lawyers' comparative view based on experience of international data protection laws and their operation and application in practice.