BIPO | Make Life Easier.

SINGAPORE

Understanding Singapore’s Personal Data Protection Act 2012 (PDPA)

With globalization and the rise of eCommerce and cross-border trading, large amounts of personal data are being collected, used and at times, transferred to third-party organizations for various reasons.

Singapore, as with many financial centres around the world has gradually put in place measures aimed at protecting personal data by recognising both (a) the rights of individuals to protect their personal data, including rights of access and correction, and (b) the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes.

It recognises both the rights of individuals to protect their personal data.

1. Singapore’s Personal Data Protection Act 2012

Personal data in Singapore is being protected by the Personal Data Protection Act 2012 (PDPA) which took effect in phases, starting with the provisions relating to the formation of the Personal Data Protection Commission (PDPC) on 2 January 2013. Provisions relating to the Do Not Call (DNC) Registry came into effect on 2 January 2014 and the main data protection rules on 2 July 2014.

It recognises both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organizations to collect, use or disclose personal data for legitimate and reasonable purposes.

Around the same time in 2018, the European Union’s General Data Protection Regulation (GDPR) also came into effect.

A quick overview of both is listed below :

Source: https://bit.ly/2kZUvpv

Description	PDPA (Singapore)	GDPR (European Union)
When did it take effect?	Do Not Call registry: 2 Jan 2014 Data protection obligations: 2 Jul 2014	25 May 2018
Who are governed by these policies?	Covers virtually all businesses in Singapore	Applies to any organization established within and outside of the EU, so long as: • the organization offers goods or services to individuals in the EU, or • monitors their behaviour within the EU • processes and holds personal data of individuals residing in the EU, regardless of the organization's location
What is it about?	"The [Personal Data Protection Act (PDPA) of Singapore governs] the collection, use and disclosure of individuals' personal data by organizations in a manner that recognises both the right of individuals to protect their personal data and the need of organizations to collect, use and disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances." Source: Singapore Statutes Online Singapore Data Protection Commission	"The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonise the data privacy laws across Europe, to protect and empower all EU citizens' data privacy, and to reshape the way organizations across the regions approach data privacy." "The aim of the GDPR is to protect all EU citizens from privacy and data breaches in an increasingly data-driven world that is vastly different from the time in which the 1995 directive was established." Source: EU GDPR European Commission

2. Use of NRIC and *other National Identification Numbers in Singapore

From 1 Sept 2019, organizations can only ask individuals for their NRIC number :

- if required by law, or
- if necessary to prove the individual's identity

*Other National Identification Numbers applies to Birth Certificate numbers, Foreign Identity Numbers and Work Permit numbers.

When to provide your NRIC	When NOT to provide your NRIC
✓ Joining an organization as a new employee	x Redemption for free parking
✓ Checking in to a hotel	x Signing up for retail membership
✓ Seeking treatment at a medical clinic / hospital	x Submitting feedback or registering interest in a product or service
✓ Subscribing to a mobile phone line	x Online purchase of movie tickets
✓ Enrolling in a private institution	x Participating in a lucky draw

To find out more, click here

3. PDPA & Businesses in Singapore

When using, collecting or disclosing personal data, organizations are required to abide by Singapore's PDPA under these nine (9) Personal Data obligations :

1. Consent Obligation	2. Purpose Limitation Obligation	3. Notification Obligation
Your organization may only collect, use and/or disclose the personal data of individuals who have consented to such collection, use and/or disclosure. These individuals must also be given the option to withdraw their consent, subject to them giving reasonable notice. Upon the withdrawal of consent, your organization must cease collecting, using and/or disclosing the personal data of these individuals.	Your organization may only collect, use and/or disclose personal data of individuals for the purpose(s) for which consent have been given by these individuals. These individuals should also not be required to consent to the collection, use and/or disclosure of their personal data beyond what is reasonable for the organization to provide a particular product or service.	Your organization should inform individuals of the purpose(s) for which their personal data is being collected, used and/or disclosed.
4.Access and Correct Obligation	**5.Accuracy Obligation**	**6.Protection Obligation**
Your organization is obliged to provide information to individuals, upon request and as soon as reasonably possible, on: What personal data of theirs is in your organization's possession or under its control; and How such personal data has been used or disclosed within 1 year of the request. Also, should an individual request that the organization rectify any error or omission in his or her personal data, your organization must accede to the request as soon as practicable.	Ensure that the personal data collected by the organization is accurate and complete.	Your organization should put in place the required security measures to protect the personal data in its possession or control. This is to prevent any unauthorised access, collection, use and/or disclosure of such data. Examples of when the protection obligation applies would be when your organization is processing and sending personal data, or disposing of documents containing personal data.
7.Retention Limitation Obligation	**8.Transfer Limitation Obligation**	**9.Openness Obligation**
Your organization should retain the personal data for only as long as is necessary for business or legal purposes.	If your organization is transferring the personal data overseas, such as storing the data in the cloud, ensure that the country to which the data is being transferred offers a comparable level of data protection as is provided by the PDPA.	Your organization should be open to sharing information about its data protection practices, policies and complaints processes upon request. For example, your organization's privacy policy can state that individuals who wish to know more the organization's data protection policies can get in touch with its data protection officer, and also provide means of contacting that officer.

Organizations found in breach of any of the data protection provisions in the PDPA, may be required to :

- Stop collecting, using or disclosing personal data in contravention of the Act;
- Destroy personal data collected in contravention of the Act;
- Provide access to or correct the personal data; and/or
- Pay a financial penalty of an amount not exceeding SGD1 million.

4. PDPA & Employers in Singapore

To help organizations and individuals better understand how the PDPA applies in the context of employment in Singapore, here are some scenarios :

a. Does an organization need to seek the consent of a job applicant for the collection and use of his/her personal data?

• When individuals voluntarily provide their personal data to an organization in the form of a job application, they are deemed to have consented to the organization collection, using and disclosing such personal data for the **purpose of assessing their job application.**

• When the individual is subsequently employed, it would be reasonable for the organization to continue using the personal data provided in the job application form for the **purpose of managing the relationship** with the individual.

• In the event the organization would like to use the personal data for purposes may not be deemed or to which there is no applicable exception under the PDPA, the organization must then inform the individual and obtain consent for such purpose.

b.How long can an organization store the personal data of job applicants who are not hired?

• This should be kept only for as long as it is necessary for business or legal purposes.

• Organizations should also note that job applicants have the right to access and request corrections to their personal data held by the organizations.

• Upon request, the organization must also inform the individual of the ways in which the personal data has been used in the **past year**.

• In the event the individual is not selected for the role, is the personal data in question is opinion data kept solely for evaluative purposes, organizations are not required such information. In this instance organsiations will not need to inform the individual of the opinions formed about them in the course of determining their suitability and eligibility for the job.

c. Can organizations use the information found in business cards for recruitment purposes?

• The PDPA does not apply to "business contact information" defined in the PDPA as an individual's
- Name
- Position name or title
- Business telephone no. or business fax no.
- Business address
- Business electronic mail address
- Any other similar information about the individual not provided by the individual solely for his personal purposes

d. How does the PDPA apply to employment records of employees?

• Organizations should inform employees of :
- Purpose of collection
- Use and disclosure of their personal data
- Obtain consent prior to the collection, use and disclosure

• In many instances, consent is obtained at the start of the relationship (at the point of appointing the new employee). Consent should be obtained at various points **during the employment relationship** when the need for more personal information is required, etc. Employees do have the option to withdraw their consent under the PDPA.

• Consent is not required if the information being collected, used or disclosed is for **"evaluative purposes"**, defined as (among other things), the purpose of determining the suitability, eligibility or qualifications of an individual for employment, promotion in employment or continuance of employment, eg :

- Obtaining a reference from a former employer to determine suitability.
- Obtaining a performance record or other relevant information to determine the performance of an employee

e. Collecting, using and disclosing personal data for the purpose of managing or terminating an employment relationship between the organization and individual

• While consent is not required by employees, employers are **required to notify their employees** of the purposes of such collection, use or disclosure although the form and manner of notification is not prescribed under the PDPA.

• For avoidance of doubt, where an organization has **sufficiently provided a general notification** to employees of the purpose for which the data will be collected, used and disclosed (eg: Performance Appraisals), it may not be necessary for the organization to notify employees of the same purpose each time the organization engages in such activities.

• Purposes that could fall within "managing or terminating an employment relationship" :
- Using the employee's bank account details to issues salaries
- Monitoring how the employee uses computer network resources and company intranet
- Managing staff benefit schemes (eg: training / educational subsidies)

• Organizations may continue to retain personal data about the former employee for as long as there is a valid or legal purpose. However, they should not retain personal data without a clearly defined purpose. They run the increased risk of a contravention of Data Protection Provisions if the data is being held on to for an indeterminate duration.

f. Organizations' responsibility if their employees do not comply with PDPA

• Organizations are responsible for any breaches caused by their employees acting in the course of their employment. In particular, any act done or conduct engaged in by an employee in the course of this employment shall be treated as done or engaged by the employer, whether it is with the employer's knowledge or approval

• PDPA defines "employees" to include a volunteer, and "employment" to include working under an unpaid volunteer working relationship.

For the full list of Advisory Guidelines on how the PDPA applies to particular issues and domains, visit: Singapore Data Protection Commission

5. Storage Security & Data Security

While not part of the PDPA, businesses in Singapore may also want to evaluate how they store, retrieve and protect personal data (whether for their employees or for other professional purposes).

• **Storage security** – keeping private information out of the hands of unauthorized personnel, which also includes protecting data from cyberattacks, ransomware, etc

• **Data security** – ensuring data remains available in the event of power outages, natural disasters, etc

*Both areas are closely related to **data protection** and may overlap. However, when looked at individually, each functions differently within the IT and Cybersecurity ecosystem.

As an organization, here are some areas to consider :

• Is your data being stored on-premise or on the cloud (i.e. through a third-party vendor)

• If data is stored on-premise :
(a) is your current IT infrastructure capable of supporting this and
(b) are there sufficient security and cybersecurity measures in place to prevent data breaches

• If data is stored on the cloud through a third-party cloud provider, what security measures are in place? Examples: independent Penetration Tests conducted annually, ISO27001 Information Security Management System Certification and other relevant certifications, etc

• In the event of power outages, are there adequate back-up measures in place to retrieve and reinstate the "lost" data. Such considerations could include back-up policies and schedules provided by third-party cloud providers

• When transferring personal data, are these encrypted for security purposes and are they compliant with the relevant PDPA and/or GDPR policies

• Other internal measures include :
- Conduct risk assessment exercise to ascertain if information security arrangements are adequate
- Use of web application firewall
- Use of anti-virus software with automatic update
- Periodic application of security updates for OS and software
- Periodic review of user access

In conclusion, organizations are required to comply with the entire Personal Data Protection Act 2012 (PDPA).

- Personal data collected before the the PDPA came into effect on 2 July 2014 (for the purposes which the personal data was originally collected) may continue to be used, unless the individual has withdrawn consent.

- Organizations must notify and obtain the individual's consent to the collection, use and disclosure of his or her personal data if such data is obtained after 2 July 2014.

About BIPO

BIPO is a leading one-stop human resources provider in Asia Pacific, focused on providing organisations with innovative ways to manage complex end-to-end HR processes. Through our cloud and mobile- based Human Resources Management system as well as industry-leading solutions such as Payroll Outsourcing, Attendance Automation, Business Intelligence, HR Consulting, Recruitment & Business Process Outsourcing and Flexible Employee Management, we help companies transform their HR operations to and beyond their expectations, while achieving business goals related to cost and profitability.

Established in Shanghai in 2004, our Asia Pacific headquarters is in Singapore and R&D centre in Indonesia. We have offices in Australia, Hong Kong, India, Japan, New Zealand, Philippines, Vietnam, Taiwan and Thailand with business links in over 10 countries and regions.
Visit www.biposervice.com and connect with us on Facebook, LinkedIn and WeChat.