“Up close and personal with data”

- is my personal data safe with my employer?

A LAWWORKS Pocket Series 2

LawWorks *is a partnership between the National Trades Union Congress and The Law Society of Singapore that aims to educate employees on their legal rights, and to promote the interests of employees generally. This booklet is part of a* ***LawWorks*** *Pocket Series intended to provide a guide to particular areas of employment law, provide a checklist of key considerations, and point the way to avenues for further advice and assistance.*

Regular legal clinics and periodic legal primers will be conducted under ***LawWorks****. For more information on legal awareness and assistance for employees, please contact the National Trades Union Congress at: LawWorks@ntuc.org.sg or The Law Society of Singapore at: LawWorks@lawsoc.org.sg.*

Disclaimer

This booklet incorporates all the relevant laws as at 1 September 2015

Acknowledgement

The National Trades Union Congress and The Law Society of Singapore wish to express our heartfelt gratitude to Ms Susan de Silva, Partner of Bird & Bird ATMD LLP, for agreeing most readily to co-write this ***LawWorks*** Pocket Series "Up close and personal with data - is my personal data safe with my employer?". Her expertise in this field is reflected in this concise guide which will enable employees in Singapore to understand the technicalities of the data protection legislation and their rights as employees.

CONTENTS

1. Introduction and Overview of the Personal Data Protection Act

1.1 Purpose of guide

This guide provides an overview as to how your personal data as an employee is protected under the Personal Data Protection Act (PDPA).

As an employee, you will be asked for your personal data by your employer for purposes connected to your employment or the employer's business, such as for paying your salary into your personal bank account, managing medical benefits, or for security systems within the company. Even before you start working, your employer may have asked you to fill out an application form with your personal details such as your education history, previous employment history and perhaps the names of your family members. It is also possible that your former employer will have retained some of your personal data for certain purposes, such as for reference for future vacancies.

Generally, your personal data should be collected, used and disclosed (sometimes referred to for short in this guide as "**processed**") for a specific purpose, for which your consent is generally required unless the situation falls under a consent exemption in the PDPA (see *Sections 3.1.3 and 3.1.4* below).

The PDPA provides for when your employer must obtain your consent to process your personal data, the limits on such processing, and your rights regarding your personal data which is held by your employer.

1.2 PDPA principles on employee personal data protection

The main PDPA principles which relate to your personal data as an employee are as follows:

- **Consent.** Your employer must obtain your consent to collect, use and disclose your personal data. However, there is a broad exception to this general rule – your employer need not seek your consent to collect, use and disclose your personal data for the purposes of "managing and terminating your employment" so long as it notifies you that it is processing your personal data for this purpose.

Notwithstanding this exemption, your employer may nevertheless seek your consent to collect, use and disclose your personal data as an employee.

- **Purpose.** Your personal data can only be processed for the purpose for which it was collected, and the purpose must be "reasonable".
- **Notification of purpose.** You must be notified of the purpose for which your personal data is to be collected, used and disclosed.
- **Access to & correction of your personal data.** You may ask your employer to (i) allow you to see your personal data and (ii) correct your personal data. Your employer will then need to update 3rd parties (for example, benefits providers) to whom your personal data has been provided in the last 12 months.
- **Accuracy of your personal data.** Your employer must make a reasonable effort to ensure that your personal data is accurate and complete.
- **Protection of your personal data.** Your employer must put in place reasonable security measures to protect your personal data against unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

- **Retention of your personal data.** Your employer must not retain your personal data when your personal data is no longer required for the purpose for which it was originally collected, unless your employer has business or legal reasons to retain your personal data.
- **Transfer of your personal data.** If your employer transfers your personal data out of Singapore, your employer must put in place measures to ensure that overseas organisation which receives your personal data provide a standard of protection comparable to the Singapore PDPA.
- **Openness.** This principle requires your employer to develop and implement data protection policies and complaint processes and to make such policies, practices and processes publicly available, including to employees.

These principles are briefly discussed in *Section 3* below.

1.3

Employees' liability under the PDPA

The obligations under the PDPA to protect personal data is imposed on organisations (whether located in or outside Singapore) which collect, use or disclose personal data in Singapore.

As an employee, you have no personal liability under the PDPA. However, your employer can be liable for your acts. If your actions or conduct in the course of your work cause your employer to breach the PDPA, your employer will be liable to be prosecuted for the breach of the PDPA, unless your employer is able to raise a defence that it has taken practicable steps to prevent you as an employee from taking such actions or engaging in such conduct.

However, if you are also an officer of your employer company, in addition to causing your employer to be liable, you too may be liable if the breach is proved to have been committed with your consent or connivance or is attributable to your negligence. In that case, you will be liable to be prosecuted and punished to the same extent as your employer company (see *Section 4.1* below for the penalties).

An "officer" means a director, partner, member of the committee of management, chief executive, manager, secretary or other similar officer of the employer company and includes any person purporting to act in any such capacity.

You may, however, be liable to your employer based on other legal duties owed to your employer which are outside of the PDPA, such as under your employment contract or other common law rules.

2. DEFINING "PERSONAL DATA"

2.1 What is "Personal Data"?

In general, any data about you is personal data if you can be identified from that data. Such data can range from your name and contact numbers to other types of data that form part of your personnel record.

Personal data under the PDPA may include any of the below, or a combination of them:

- Full name
- NRIC or passport number
- Residental address
- A person's photograph or video image.
- Mobile telephone number.
- Personal email address.
- Thumbprint.
- DNA profile.

Generic information that does not identify a particular individual is not personal data. However, generic information can become part of an individual's personal data when combined with personal data or other information which enables that individual to be identified.

Example #1

Mary is a female Singaporean of 18 years of age. Such general characteristics as "female", "Singaporean" and "18 years of age" are not by themselves usually capable of identifying an individual and so are not in themselves personal data.

However, when Mary fills up an employment application form with her full name, NRIC number, gender, nationality and age, all the information on the form, including the general characteristics, constitutes Mary's personal data, since the information when taken together will be capable of identifying Mary.

2.2

Excluded Personal Data

Certain types of information by which an individual can be identified are not treated as "personal data". Key examples include:

- **business contact information** that you provide for business purposes, and not solely for personal purposes. Whether or not your personal details are business contact information therefore depends on the purpose for which you provide your business contact details.

Example #2

John works for ABC Pte Ltd. He gives out his business name card to everyone that he meets for business networking purposes. The information on his card will be considered business contact information and not "personal data". If John gives out his business name card solely for his personal purposes for example, to register for personal gym package, the information on his card will be his personal data protected by the PDPA, and not merely business contact information.

- **publicly available information**

Example #3

John is a member of an online social network. His membership profile has his profile picture, name, date of birth, education and employment history which is publicly searchable. The data on John's social network page is likely to be personal data that is publicly available, since any other member of the public will be able to access his personal data.

Example #4

Mary is also a member of the same online social network. However, Mary's membership profile is restricted to a closed circle of family and friends to whom she has granted permission to access her profile. The personal data on Mary's social network page is less likely to be considered publicly available since access to her personal data is limited.

3. KEY PDPA PRINCIPLES

3.1 Consent

3.1.1 Giving your consent

In general, your personal data can be collected, used or disclosed by your employer only with your consent. Your consent can be obtained in a number of ways – for example, in writing or verbally.

Example #5

John attends a course that his employer has sent him on and writes his name and mobile number in a registration book for attendance purposes. A recruiter who attends the same course sees John's contact details in the registration book. The recruiter takes down John's details and later calls John to ask if he is keen to explore other job opportunities. This is potentially a violation of the PDPA, as the recruiter has collected and used John's personal data without his consent.

3.1.2 Deemed consent

There are two situations in which you may be deemed to have given your consent for your personal data to be

processed, even if you have not explicitly given your consent:

- Where you **voluntarily provide** your personal data for **a purpose** without actually giving consent, and it is **reasonable that you would voluntarily provide** your personal data for that purpose.

Example #6

John orders a meal at a cafe, and hands his credit card to the cashier. The cashier need not ask for John's consent to process the payment as John has voluntarily given his credit card and it is reasonable that John has consented for the personal data on his credit card being disclosed to the cafe for the purpose of processing the payment.

- Where you consent to the **disclosure** of your data **from Party A to Party B** for a purpose, you will be deemed to have consented to the collection and processing of your personal data by Party B for that purpose.

Example #7

John is injured at work and an ambulance arrives to take him to hospital for treatment. On the way to the hospital, the ambulance attendant asks John about his medical history and his injury and then provides those details to the doctors at the hospital. Although John has not given consent for the ambulance attendant to give this information to the doctors, it is reasonable for the ambulance attendant to assume that John would like to be treated by doctors at the hospital who are aware of John's medical history.

3.1.3 Consent exemptions

There are certain important consent exemptions which allow your employer to collect, use and disclose your personal data without your consent e.g.:

- To manage or terminate your employment relationship (with notification of this purpose – see *Section 3.1.4* below).
- For evaluative purposes e.g. to assess your suitability, eligibility or qualifications for hire, promotion or removal from employment or office.
- To respond to an emergency threatening the life, health or safety of an individual.
- If obtaining your consent is inconsistent with other written laws.

3.1.4 Consent exemption - managing or terminating an employment relationship

This is a key consent exemption in the employment context. Although your consent is not required for the purposes of managing or terminating the employment relationship, the employer must still notify you in advance that your personal data will be processed for the purposes of managing or terminating your employment relationship and must ensure that the collection, use and disclosure of your personal data is reasonable for the purposes of managing or terminating an employment relationship.

The phrase "managing or terminating an employment relationship" is not defined in the PDPA. According to Advisory Guidelines by the Personal Data Protection Commission ("**PDPC**"), purposes that could fall within this consent exemption include:

- Using an employee's bank account details to pay salary;
- Monitoring how an employee uses company computer network resources;

- Posting employees' photographs on the staff directory page on the company intranet; and
- Managing staff benefit schemes such as training or educational subsidies.

However, given that the full scope and meaning of "managing or terminating an employment relationship" is not completely clear, employers may prefer to obtain their employees' consent to process their personal data for employment and business purposes, instead of relying on this consent exemption.

3.1.5 Disclosing employees' personal data to unions

During a recent parliamentary debate, the Minister for Communications and Information clarified that an employer may rely on the consent exemption of "managing or terminating an employment relationship" to disclose the personal data of employees who are union members to the unions to allow the unions to carry out their duties in representing the employees, for example, in the case of retrenchment. It is thus not necessary under the PDPA for employers to obtain their employees' consent to disclose their personal data to unions which have been

recognised by the employers to enable the unions to represent the employees who are union members. The Minister also clarified that employees must be informed that their personal data may be collected, used and disclosed for such purposes and suggested that the employees be notified by HR as part of the organisation's general HR policy or that such notification be included in the employment terms.

3.1.6 Third Parties' personal data

Where personal data of your family member(s) for benefits administration or other third parties such as your referees will be collected, used or disclosed, the employer should ensure that consent of the employee's third parties has been obtained before collecting, using or disclosing such third parties' personal data. For this reason, the employer may obtain a written confirmation from you that you have obtained the consent of such third parties whose personal data you are providing to your employer.

3.1.7 Withdrawing your consent

You have the right to withdraw your consent by giving reasonable notice to your employer. Your employer must then inform you of the likely consequences of such withdrawal.

If you withdraw your consent, your employer must stop collecting, using and disclosing your personal data, unless the collection, use or disclosure of your personal data is required or permitted under the PDPA or any other written law.

In the employment context, it is likely that the consequence of withdrawing your consent to your employer collecting, using and disclosing your personal data is that your employer may no longer be able to administer your employment and thus may no longer be able to employ you, unless the employer is able to rely on the consent exemption for "managing or terminating an employment relationship".

Example #8

John resigns from his position with ABC Pte Ltd. On his last day, John informs ABC that he withdraws his consent from ABC using his personal information for any purpose. ABC must now stop collecting, using & disclosing John's personal data except for the purpose of administering the process of terminating the employment relationship, or for legal compliance such as tax filing.

3.2 Purpose

Your employer may collect, use or disclose personal data about you only for purposes that a reasonable person would consider appropriate in the circumstances of your employment, and about which purposes you have been informed by your employer.

Example #9

Mary is asked by her employer to give her birthdate, age, weight, blood type and marital status without being told the purposes for this request. In this case, if Mary does provide such information, the employer will be in breach of the PDPA for collecting personal data without informing Mary of a reasonable purpose for this request.

Example #10

Mary is asked by her employer to give her birthdate so that the company can organise an "office-wide birthday celebration" for all employees' birthdays which fall within the same month. In this case, the employer is likely to be considered to have notified Mary of a reasonable purpose for collecting her personal data.

Example #11

Mary's manager insists that Mary tells the manager her age as the manager has an unreasonable personal bias against workers above a certain age being able to do the job. In this case, if Mary discloses her age, the employer (through the manager's action) is not likely to qualify as having a reasonable purpose for collecting such personal data.

Example #12

John is asked by his employer to provide contact details of his family members. When John asks why, he is told that such information is needed for emergency contact purposes only. John provides his wife's contact details. A few days later, John finds out that his wife has been contacted by his employer's sales department to market some products to her. This is potentially a violation of the PDPA as the employer has collected, used & disclosed John's wife's personal data for a different purpose, and not for marketing purposes.

3.3

Notification of Purpose

On or before collecting, using or disclosing your personal data, you must be notified by your employer of the purpose(s) for which your employer intends to collect, use or disclose your personal data.

Example #13

Mary is at work when an HR representative hands her a form and asks her to complete the form which requests details of Mary's personal data. When Mary asks what the form is for, the HR representative says that the form is "for the company". In this case, the employer is not likely to have notified Mary of the purpose for which her personal data is being collected.

Example #14

HR circulates an email requesting for employees' postcode for the company's statistical purposes. In this case, the employer company would be considered to have stated a sufficiently specific purpose.

There are certain situations under the PDPA where notification is not required, such as where:

- you are deemed to have consented (see *Section 3.1.2* above), or

- the personal data is collected to respond to an emergency that threatens the life of an individual (see *Section 3.1.3* above).

3.4 Access to & correction of your personal data

Upon your request, your employer must:

- give you access to your personal data which is in the possession or under the control of the employer;
- correct any error or omission in your personal data as soon as practicable;
- send the corrected data to every other organisation to which the personal data was disclosed by your employer within a year before the correction, unless your employer considers that such correction is not needed.

However, your employer must not provide you access to your personal data if doing so may:

- cause immediate or grave harm to your safety or physical or mental health;
- threaten the safety or physical or mental health of another individual;
- reveal personal data about another individual;
- reveal the identity of the person who has provided the personal data about you, and the person has not consented to the disclosure of his/her identity; or

- be contrary to national interest.

There are other exceptions where your employer is not required to provide access and make the correction, for example, where opinion data is kept solely for an evaluative purpose.

Your employer is entitled to levy a reasonable charge for an access request, but must not charge you for a correction request.

Example #15

John is looking at his company's intranet when he notices that there is an error in his job title. He contacts his employer and asks for the error to be corrected. Under the PDPA, the employer must correct the personal data as soon as practicable.

3.5

Accuracy of your personal data

An employer must make a reasonable effort to ensure that personal data collected by or on behalf of the employer is accurate and complete if:

- the personal data is likely to be used by the employer to make a decision that affects you; or
- the personal data is disclosed by the employer to another organisation.

Example #16

ABC Pte Ltd sends out an annual email alert to all staff to remind them to update their personal details particularly their new certification/ qualifications (if any) on the intranet. ABC Pte Ltd is likely to have met its obligation to update its employees' personal data.

3.6 Protection of your personal data

An employer must protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

Example #17

ABC Pte Ltd keeps its personnel files in an unlocked cabinet in an open area of its office entrance. This arrangement is not likely to constitute "reasonable security arrangements" as there is no restricted access to the personal data in the files.

Example #18

ABC Pte Ltd buys a secure safe for its personnel records and places it in the HR administration room, with only the HR Manager and selected HR staff having access to the safe via a confidential password. This arrangement is likely to be considered a reasonable security arrangement as access to the personnel files is limited to the appropriate personnel.

3.7

Retention of your personal data

An employer must not retain employees' personal data as soon as:

- the purpose for which the personal data was collected is no longer served by retaining the personal data, and
- retention is no longer necessary for legal or business purposes.

Example #19

John has worked for his company for over 20 years and the company still keeps his records from the late 80's "just in case" such records may be needed in the future. Unless the company has any legal or business reason to retain John's old records, this may not in itself be a valid purpose and the company must cease retaining such personal data.

3.8

Transfer of your personal data

If your employer transfers your personal data out of Singapore, for example, to a centralised shared HR services function within your employer's group of companies, your employer must put in place measures to ensure that overseas organisation which receives the personal data provide a standard of protection which is comparable to the Singapore PDPA.

3.9

Openness

An employer must develop and implement data protection policies and complaint processes, communicate to its employees such policies and complaint processes, and make such policies and complaint processes publicly available upon request.

An employer must also designate at least one person as a "data protection officer" to be responsible for ensuring that the company complies with the PDPA, and make publicly available the data protection officer's business contact information.

4. VIOLATION OF PDPA

4.1 Enforcement

Financial penalties of up to S$1 million may be imposed on the employer company for breaching the PDPA.

If your actions in the course of your work cause your employer to breach the PDPA, your employer will be responsible for the breach (see *Section 1.3* above).

Individuals who have suffered loss as a result of a breach of the PDPA may also bring a private right of action against the responsible company.

4.2 How to Report a Personal Data Protection Concern

The PDPC encourages parties to resolve personal data protection concerns through communication before filing a complaint with the PDPC. This is because organisations are usually in the best position to provide clarity on their data protection policies and reasons for handling an individual's personal data in a certain manner.

If you wish to file a complaint with the PDPC, you will find the relevant forms and steps at: https://www.pdpc.gov.sg/individuals/complaints-and-reviews/report-a-personal-data-protection-concern/personal-data-protection-complaint

Upon receiving your complaint, the PDPC will consider whether it might be more appropriate to resolve it by informing the organisation to contact you regarding your concerns. If the matter cannot be resolved directly, the PDPC may refer the matter for mediation by a qualified mediator. The PDPC will only do so if both you and the organisation agree to mediation.

5. Checklist and other tips

- Think about why your employer is asking for your personal data. If it is not clear why they need it, ask your employer.
- If your employer cannot give you a good reason as to why it wishes to collect that personal data, you may decide not to give your consent to your employer. However, your employer will then inform you of the consequences of not consenting, which may include the inability to continue employing you.
- You may revoke your consent at any time. In the event you do so, your employer must cease collecting, using and disclosing your personal data and must inform you of the consequences of you withdrawing your consent.
- Ensure you know why your employer retains personal data. If there is no legal or business reason to retain it, or the purpose no longer exists, your employer must cease collecting, using and disclosing your personal data.

For more assistance / information

- If you are a union member, you may:
  - approach U PME Centre at NTUC Centre, 1 Marina Boulevard, #B1-01 NTUC Members' Hub, One Marina Boulevard, Singapore 018989
  - email to pme@ntuc.org.sg
  - visit PME Portal at www.ntuc.org.sg/pme

- You may also:
  - approach the Pro Bono Services Office of The Law Society of Singapore at 50 Market Street, #10-04 Golden Shoe Car Park,
  - Singapore 048940.
  - call the general line at 6536 0650
    email to probonoservices@lawsoc.org.sg

Join NTUC Professionals, Managers and Executives' (PMEs) Conversations online:


www.facebook.com/UPforPMEs


www.linkedin.com/groups/UP-PMEs-4573957


www.twitter.com/UPforPMEs

LAWWORKS

A PARTNERSHIP BETWEEN

ntuc
National Trades Union Congress

THE LAW SOCIETY OF SINGAPORE