PDPA & DNC REGISTRY

Posted on August 1, 2014

Category: CNPupdates

General disclaimer

This article is provided to you for general information and should not be relied upon as legal advice. The editor and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents.

Date Published: 1 August 2014

Authors: Wong Pei-Ling, Stephen Soh and Paul Yap.

With the main personal data protection provisions coming into effect on 2 July 2014, we highlight some salient legal information you should know in protecting your personal data.

What is personal data?

Personal data is defined in the Personal Data Protection Act 2012 ("**PDPA**") as "data, whether true or not, about an individual who can be identified:

- from that data; or
- from that data and other information to which the organisation has or is likely to have access".

The Personal Data Protection Commission (the "**PDPC**") describes the PDPA as establishing "a data protection law that comprises various rules governing the collection, use, disclosure and care of personal data. It recognises both the rights of individuals to protect their personal data, including rights of access and correction and the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes". The scope of the PDPA in general covers personal data held by any organisation (company, partnership, sole trader, society, charity, etc.) and would include information such as an individual's name, image, telephone numbers, personal email address and residential address.

As part of our daily lives, we frequently give personal data to various organisations (either by filling up forms at boutiques, supermarkets and other stores or on-line when purchasing things, applying for credit cards or store "VIP" or discount cards or signing up on websites) which in turn may (and often do) share the personal data with other organisations or may use it for other purposes other than the original purpose for which you had provided it. For example, when you purchase large items from a department store, you will have to divulge your name, contact details and address for delivery and the store will pass on that personal data to the delivery company. Whilst the purpose for which you had provided the personal data was to enable delivery, subsequently and all too often, you may get an SMS, email or leaflet from the store promoting new items or sales or from the store's bank inviting you to apply for a credit card.

What you need to know about the Spam Control Act and the Personal Data Protection Act

The Spam Control Act ("**SCA**") seeks to address the problem of unsolicited commercial bulk messages sent indiscriminately. The SCA sets out a framework to manage spam (unsolicited commercial electronic messages sent by organisations to consumers by electronic mail or text messaging). The SCA requires organisations to, inter alia, include an "<ADV>" label in the header in the subject field of the electronic message, or where there is no subject field, as the first words in the message, and to provide an unsubscribe facility within the spam message.

General disclaimer

This article is provided to you for general information and should not be relied upon as legal advice. The editor and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents.

While the SCA provides for the control of spam messages, the PDPA works in tandem with the SCA to set out the rules governing the proper collection, use and disclosure of personal data by organisations thus providing a measure of protection to the consumer by imposing certain restrictions on the collection and use of personal data by organisations and restricting the sending of unsolicited spam. However, the data protection obligations in the PDPA do not apply to any public agency or an organisation that is acting on behalf of a public agency, in relation to the collection, use or disclosure of the personal data. A "public agency" includes the Government (including any ministry, department, agency or organ of State, any tribunal appointed under any written law, or statutory body).

The PDPA is being introduced in stages. Provisions relating to the PDPC were introduced on 2 January 2013, while the provisions pertaining to the Do Not Call Registry were introduced on 2 December 2013 as well as 2 January 2014. With the main data protection rules of the PDPA pertaining to the collection, use, disclosure, access and correction, and care of personal data coming into force on 2 July 2014, you will have more control over how your personal data is handled by businesses and other organisations. You can decide which organisations can collect your data, how it is to be used, and whether it can be disclosed to another organisation. The PDPA also gives you rights of access and correction in relation to your personal data kept by organisations.

You will still have a responsibility to protect your own personal data. By being aware of your rights and the obligations of the organisations, you can reduce the risks of misuse of your personal data by organisations.

We highlight three salient points that you should know about the PDPA.

Collection, use and disclosure, including withdrawal of consent

- For personal data that organisations collect before the main data protection rules of the PDPA come into effect i.e. 2 July 2014, organisations may continue to use such personal data for the purposes for which it was collected unless you inform the organisations that you do not consent to their use of your personal data. For personal data that organisations collect after 2 July 2014, organisations have to get your consent to the collection, use and disclosure of your personal data. The organisations should inform you of their purpose(s) for collecting, using and disclosing your personal data.
- Organisations should not make it a condition that you consent to the collection, use and disclosure of your personal data beyond what is reasonable to provide a product or service to you. If you voluntarily provide your personal data to an organisation for a particular purpose, you may be considered to have consented to the use of your personal data for that specific purpose.
- You are free to withdraw your consent for the collection, use and disclosure of your personal data by an organisation at any time by giving reasonable notice. The organisation should inform you of the likely consequences of your withdrawal of consent (e.g. whether the organisation will be able to continue providing you the product or service), and cease collecting, using or disclosing your personal data.

General disclaimer

This article is provided to you for general information and should not be relied upon as legal advice. The editor and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents.

Access and Correction

- You can request the organisation to grant you access to your personal data that the organisation possesses, for information about the ways in which your personal data has or may have been used or disclosed within a year before the request, and for the organisation to correct any errors or omissions in your personal data. The organisation should also send the corrected data to other organisations to which it has disclosed the incorrect data.
- However, organisations are prohibited from granting you access to your personal data under certain circumstances such as if the disclosure would cause immediate/serious harm to yourself or someone else, reveal someone else's personal data, or be contrary to the national interest.

Care of Personal Data

- Organisations should make reasonable efforts to ensure that your personal data kept with them is accurate and complete, make reasonable security arrangements to protect your personal data and to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.
- Once your personal data is no longer necessary for legal or business purposes, the organisation should stop keeping your personal data.
- However, there are some exceptions to these rules such as exceptions relating to emergency situations, investigations, publicly available data or where personal data is used for evaluative purposes.

What you need to know about the Do Not Call Registry

A national Do Not Call Registry, commonly known as the DNC Registry, has been set up with effect from 2 January 2014 for you to register your Singapore telephone number if you do not wish to receive telemarketing calls, messages and/or faxes from organisations. The DNC Registry is managed by the PDPC.

If you do not wish to receive unsolicited telemarketing calls, messages and/or faxes, you may register your Singapore telephone number with any or all of the 3 registers:-

- No Voice Call Register: Register your Singapore telephone number here if you do not want to receive unsolicited telemarketing phone calls.
- No Text Message Register: Register your Singapore telephone number here if you do not want to

General disclaimer

This article is provided to you for general information and should not be relied upon as legal advice. The editor and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents.

receive unsolicited telemarketing text messages.
- No Fax Register: Register your Singapore telephone number here if you do not want to receive unsolicited telemarketing faxes.

How to register

You may add your Singapore telephone number to any or all of the DNC Registers at any time. Registration is free and does not expire unless you deregister or terminate your Singapore telephone number.

There are three methods to register. You may register at the DNC Registry's website, by SMS, or by calling the DNC Registry. Detailed instructions on how you may register your Singapore telephone number may be found at www.dnc.gov.sg.

Effect of registration

You should expect to stop receiving unsolicited telemarketing messages through your registered Singapore telephone number 30 days after registration (if you register on or after 2 July 2014), or up to 60 days after registration (if you register before 2 July 2014).

If you want an organisation to send you telemarketing messages in spite of you registering your Singapore telephone number with the DNC Registry, you may simply give the organisation your consent directly. The organisation may then send marketing messages to your Singapore telephone number even if you have added your Singapore telephone number to the DNC Registry. This enables you to be selective about which organisations may contact you.

Deregistration

Your registered Singapore telephone number will remain on the DNC Registry unless you terminate your Singapore telephone number or you deregister your Singapore telephone number from the DNC Registry. You are free to deregister your Singapore telephone number from the DNC Registry at any time.

Lodging a complaint

If, after you have registered your Singapore telephone number with the DNC Registry, you suspect that an organisation has breached the DNC provisions (e.g. by sending you telemarketing messages), you may contact the organisation sending you the telemarketing messages to clarify your concerns on whether your personal data has been misused, request that they stop doing so, or you may wish to lodge a complaint with the PDPC.

Below are some guidelines provided by the PDPC on their website to help you in deciding when you may

General disclaimer

This article is provided to you for general information and should not be relied upon as legal advice. The editor and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents.

make a complaint:-

- Was the telemarketing fax, text message or call sent to you within the first 60 days of adding your Singapore telephone number to the DNC Registry?
- Have you previously given clear consent to the organisation to send you telemarketing calls, text messages or faxes, and that consent has not been withdrawn?
- Is the message or call excluded from the scope of the DNC Registry provisions? For example, it would be excluded if it was sent by a public agency under, or to promote a programme carried out by that public agency which is not for a commercial purpose or solely to conduct market research or survey or for offering you an employment opportunity?
- Is the call, text message or fax for Business-to-Business telemarketing? For example, is the telemarketer trying to sell corporate insurance to your company?

You may wish to consider filing a complaint if you have answered "no" to all of the above.
The guidelines on the PDPC website also explain that if you receive an unsolicited text message or fax, you may also wish to consider the following additional questions reproduced from the PDPC website:-

- Do you have an ongoing relationship with the organisation sending the text message or fax?
    1. Yes (Please proceed to question 2 below)
    2. No (You may wish to lodge a complaint)
- Is the purpose of the fax or text message related to the subject of the ongoing relationship?
    1. Yes (Please proceed to question 3 below)
    2. No (You may wish to lodge a complaint)
- Have you withdrawn your consent, opted out more than 30 days ago through an opt-out notice, or indicated to the sender that you do not consent for the sender to send you marketing text or fax messages?
    1. Yes (You may wish to lodge a complaint)
    2. No (You may wish to contact the organisation to inform them that you withdraw your consent, opt-out, or inform the sender that you do not consent for the sender to send you marketing text or fax messages)

If you have assessed the situation based on the guidelines from the PDPC website reproduced above, you may lodge a complaint to the PDPC. Please note that all complaints will be subjected to an initial screening to identify whether there are any potential breaches of the PDPA.

Conclusion

We hope this article is helpful in creating awareness of your new legal rights under the PDPA and the SCA.

General disclaimer

This article is provided to you for general information and should not be relied upon as legal advice. The editor and the contributing authors do not guarantee the accuracy of the contents and expressly disclaim any and all liability to any person in respect of the consequences of anything done or permitted to be done or omitted to be done wholly or partly in reliance upon the whole or any part of the contents.