What construes Personal Data? Am I protected?

Personal Data can be widely construed as any personal information of an identified person. It is shared, transferred and used by various parties who have received it. However, not many are aware of how vulnerable we are to a breach of our own personal data by data users and third-party users.

Finally, the Personal Data Protection Act 2010

After the long wait where Parliament had on many instances tried to enact an Act to protect the personal data of individuals, our very own Personal Data Protection Act 2010 ("**PDPA**") came into force on 15 November 2013.

Under PDPA, any person or company that holds any personal data or controls or has authority to process over any such information and data is known as a Data User. Data Users are responsible to ensure that the data processor, third party users, provides sufficient protection to the data that is being used.

Data Users owes the duty of care to the Data Subjects, who own these personal data and who have entrusted them with their personal data. PDPA not only protects individuals but applies and affects everyone from customers, to employees and even to third party service providers.

The PDPA is applicable to personal data in respect of **commercial transactions**. The term 'commercial transaction' gives a broad definition whereby it affects any person whether it is contractual in nature or not. This includes matters which deals with the supplying or exchanging of goods or services, investments, banking and insurance and agency. In other words, your personal information that is provided to your telco / insurance provider or even to a security checkpoint are all protected under PDPA!

By providing our personal data, it makes us the Data Subjects, the person or company who receives our data would then be the Data User while anyone else who process, further receives or is authorised to use it, is a data processor. Data Users are not supposed to share any of those data with unauthorised parties without the consent of the Data Subjects, failing which, they are would be breaching PDPA.

What can I do if I found that my Personal Data has been misused?

If this occurs, complaints can be lodged to the Department of Personal Data Protection which comes under the Ministry of Communication and Multimedia.

According to s.104 of the Act, individuals are allowed to file complaints to the Personal Data Protection Commissioner ("**Commissioner**") who is appointed to oversee the implementation of PDPA. The Commissioner would then investigate on the complaint and if the Commissioner has reasonable grounds to believe that the law had been contravened, the Commissioner may carry out investigation on the Data User.

But, the Commissioner may refuse to investigate if the act, practice or request is trivial or was not made in good faith. So come clean!

How effective is the PDPA?

PDPA came into full force in 2013 and saw its first case in 2017 when a college operator went against the Act.

The College had in 2016, processed the personal data of its former employee without a certificate of registration issued by the Commissioner. You may wonder, is it necessary to have such a certificate when dealing with the personal data of a person? **The answer is, YES!**

Anyone found to have not complied with issuing a certificate of registration is punishable under the PDPA with a maximum fine of RM500,000.00 or up to 3 years imprisonment, or both, if convicted. Data Users should make an application to the Commissioner for a certificate of registration to be issued.

Personal data is vulnerable, and it is crucial that they are protected from being unlawfully exposed. Just earlier this year, over 440,000 personal details of organ donors were leaked online. The case was not just a mere investigation by the Commission but was also investigated by the police under the Federal Commercial Criminal Investigation Department.[1]

Large scale personal data leak is happening silently and rampantly with the latest being an exposure in June this year of the Education Ministry's school exam analysis system which was exploited by hackers. This exploitation allows hackers to gain access to 4.9 million personal details of students and their parents', including their Identity Card numbers. Ten thousand schools nationwide, both national primary and secondary schools, are vulnerable to the breach of their students and parents' personal data caused by the hacking.[2]

Globally, personal data breach is not alien to many with big exposures such as the Cambridge Analytica's data-sharing scandal that had caused millions of personal data to be exposed and misused.

Sandy Parakilas, the former platform operations manager at Facebook who was responsible for policing data breaches by third-party software developers had reminded and even warned senior executives of Facebook that a lack of data protection would risk a major breach. True enough, in 2018, the scandal was exposed, alerting people around the world that their personal data might have been collected by Cambridge

[1] http://www.thesundaily.my/news/2018/01/24/personal-data-protection-commission-probe-data-leak

[2] https://www.themalaysianinsight.com/s/53835

Analytica through Facebook, sparking great outcry around the world about their personal information.

> Parakilas during an interview with The Guardian had said "*It has been painful watching, because I know that they could have prevented it.*"[1]

Breach of personal data can be preventable. It is thus crucial that data users take extra precautions and constantly improve their software security to avoid such avoidable errors.

Be aware of your rights!

As data users, every corporate must hold a higher duty of care in ensuring that the personal data of their clients are well protected against such incidents. The public too, must understand if their personal data has been used by any unauthorised party, they, as the owners of the personal data, have a right to report such incidents.

It is pertinent to know that as owners of these personal data, you may withdraw your consent to process your personal data by a mere written notice. A Data User would commit an act if he continues to process the personal data after the withdrawal of consent by you. This offence if convicted, is liable to a fine not exceeding RM100,000.00 or an imprisonment for a term not exceeding 1 year or both.

We should also be aware that under the PDPA, data users have a limit to their disclosure of data subjects' personal data. Data users may use the information for other purposes only if the data subject gives consent to disclose for the purpose to prevent or detect crime or for investigation purposes.

Furthermore, data users should not process any sensitive personal data. Such personal data comprises information as to the physical or mental health or condition of the data subject, political opinion or religious belief of the data subject, unless the data subject gives clear consent that it is for obtaining legal advice, establishing, exercising or defending legal rights, or for the administration of justice. If in contravention, the data user would be liable to a fine not exceeding RM200,000.00 or imprisonment for a term not exceeding 2 years or both.

Data users must not only ensure that the data subjects' personal data are well protected, they will have to ensure that they keep and maintain a record of any application, notice, request or any other information relation to personal data that has been used or is being processed by the data users.

The PDPA further gives a rather wide protection whereby a person who knowingly or recklessly, without the consent of the data user, collects, sells, or disclose personal data of a data user would be deemed to have committed an offence and if convicted, is liable to a fine not exceeding RM500,000.00 or an imprisonment for a term not exceeding 3 years or both. Nevertheless, informers of a breach to the PDPA is given protection under s.140 of the Act.

Be on the know on where your data has gone

Malaysians should be rest assured that while the PDPA gives protection on privacy data regarding commercial transactions, they are also protected under the common law privacy – informational privacy, that gives individuals a right to have control over their personal information.

With both the PDPA and common-law protection, Malaysians should be aware and be relieved that their personal data are protected. So, know where your data has gone!

All information in this Newsletter is correct as at **30 June 2018 unless otherwise stated.*

****

The author to this newsletter is Clarence Tan. Clarence is currently undergoing his internship with Donny & Ong.

CONTACT US

| **T** +603 6211 1316
| **F** +603 6211 1876
| **A** A-2-10, Plaza Damas 3, Jalan Sri Hartamas 1, 50480 Kuala Lumpur
| **W** www.donnyong.com
| **E** admin@donnyong.com

DONNY & ONG
ADVOCATES AND SOLICITORS
柯王律师事务所