CONTRIBUTED CONTENTS

Article from Data & Privacy SIG

Understanding and Operationalizing Singapore's Mandatory Data Breach Regime

Steve Tan†, Professor (Adjunct)
Partner, Rajah & Tann Singapore
Director, Rajah & Tann Technologies
Director, Rajah & Tann Cybersecurity

A. Introduction

1. Concomitant with the digitalisation of the world economy, organisations have in the last several years pivoted their operations and business practices to one focused on the leveraging of technology. This has brought about a tsunami of data, being generated and relied upon by organisations. Much of such data comprise personal data, i.e. in simplified words, data that directly or indirectly identifies an individual. Without a doubt, the digital economy is in essence a data driven economy.

2. As and from 1 February 2021, organisations subject to Singapore's overarching data protection law, the Personal Data Protection Act [1] ("**PDPA**"), are mandatorily required to notify Singapore's data protection regulator, the Personal Data Protection Commission ("**PDPC**") and/or affected individuals, upon the occurrence of a data breach if certain conditions are met.

3. This effectively means that organisations can no longer sweep data breaches under the carpet, as they have been accustomed to doing, in years past. The significance

† Partner and Deputy Head, Technology, Media and Telecommunications/Data Privacy practice group, Rajah & Tann Singapore. Steve has been appointed Adjunct Professor of the National University of Singapore, teaching "Privacy & Data Protection Law" at the law faculty. Steve co-founded and is Director of Rajah & Tann Technologies Pte Ltd. Steve also co-founded and is Director of Rajah & Tann Cybersecurity Pte Ltd. Highly regarded for his expertise in data privacy and technology law work, Steve has pioneered several data-protection-related services which organisations have found valuable. Steve has been recognised as a leading lawyer in *PLC Cross-border Media and Communications Handbook*, *Asia Pacific Legal 500*, *AsiaLaw Profiles*, *Practical Law Company Which Lawyer*, *Chambers Asia Pacific*, *Best Lawyers*, *The International Who's Who of Telecoms and Media Lawyers*, and *Who's Who Legal: Data*. Steve has been named Communications Lawyer of the Year in the Corporate Livewire 2015 Legal Awards and in Corporate Insider Business Excellence Award 2019. Steve is cited as "one of the best in the field of personal data protection" in *Legal 500* 2017 and as being "one of the gurus in the field of data protection" in *Legal 500* 2019 and as "*an icon in the data privacy arena. Has a great depth of knowledge as the subject matter expert and one of the sought after authorities in this field*" in *Legal 500* 2021. In 2022, Steve was awarded ALB Asia's Top 15 TMT Lawyers. Steve is a Certified Information Privacy Professional (Asia) (CIPP/A).

[1] Personal Data Protection Act 2012 (Act 26 of 2012).

back to top

of this mandatory data breach notification requirement under the PDPA is even more pronounced considering the fact that statutory fines under the PDPA[2] is one of the highest in Asia, and enforcement of the PDPA has been strong and efficient.

4. Any sort of data incident can befall an organisation at any point in time. No organisation is immune from suffering a data incident. It could be as simple as an employee accidentally sending an email with an attachment containing personal data of its customers or employees to a wrong recipient, a simple disclosure of email addresses of multiple recipients in the sightable 'cc' or 'to' field of an email, throwing documents containing personal data of customers in the dustbin without shredding, to a sophisticated hack by a third party threat actor. The operational question that every organisation needs to know would be whether any data incident, even the simplest, needs to be notified to the PDPC and/or affected individuals.

5. In assisting many organisations in dealing with data incidents, I have seen many organisations being befuddled by the above. This is exacerbated by the fact that the mandatory data breach notification regimes of different jurisdictions have significant differences and Singapore is no exception. Singapore's is markedly dissimilar from the European Union's General Data Protection Regulation[3] ("**GDPR**").

B. What is a data breach?

6. To answer the above, let us consider the expansiveness or otherwise of the mandatory data breach notification regime under the PDPA.

7. The first question that an organisation needs to consider would be whether the data incident falls within the definition of a 'data breach' under the PDPA. The PDPA defines a 'data breach' as :

> "*(a) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or*
>
> *(b) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.*"

8. This definition is rather expansive and will undoubtedly capture many incidents which may not fall within the definition of a data breach in other jurisdiction(s)' data protection laws. For example, under the GDPR, a data breach[4] is defined as :

[2] The increased fining formula is scheduled to come into force on 1 October 2022. This means that hitherto maximum fines of up to S$1 million, will be changed to the following : the higher of (i) S$ 1 million or (ii) up to 10% of the annual turnover in Singapore of the organisation where the organisation's annual turnover in Singapore exceeds S$10 million.
[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[4] The GDPR defines it as a 'personal data breach'.

back to top

> "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*".

9. By comparing the 2 different laws' definitions of what constitutes a data breach, one can ascertain that the definition under the GDPR is qualified and limited by the fact that there must have first been a '*breach of security*'. There is no such qualifier under limb (a) of the definition of 'data breach' under the PDPA (see paragraph **7** above), which renders the coverage of what constitutes a data breach under the PDPA wider than under the GDPR. This is just one of the differences.

10. The expansiveness of limb (a) of the definition of 'data breach' does leave some uncertainty though. For example, this limb captures a situation where there has been unauthorised 'use' of personal data. Read literally, could it be argued to include a situation where existing personal data of individuals that had been lawfully collected by an organisation, is being used for a purpose which is not covered by the consent previously provided by the individuals or for which no exception to the requirement of consent under the PDPA applies? If this interpretation were to be adopted, it could make the definition of 'data breach' under the PDPA even wider than as described above, as it covers not only incidents where there is the element of a breach or compromise but one where it is simply a breach of the Consent Obligation under the PDPA. Was this intended by the parliamentary drafter of the mandatory data breach notification regime?

C. Notification thresholds

11. Setting aside the uncertainty described at paragraph **10** above, there is a zone of certainty with respect to certain types of data incidents that would clearly fall within the definition of 'data breach' under the PDPA. Hence, this therefore means that many data incidents would be captured by the PDPA's definition of a data breach. Certainly, the examples given at paragraph **4** above would be captured by the definition of a 'data breach' under the PDPA, so long as the data that has been affected includes personal data. Fortunately, regardless that a simple data incident may fall within the definition of a 'data breach' under the PDPA, there is a second step to be satisfied before the requirement to notify the PDPC and/or affected individuals kicks in. This is that the data breach must meet one of the two notification thresholds under the PDPA.

12. The two notification thresholds are :

    (a) Where the data breach results in, or is likely to result in, significant harm to an affected individual ("**Notification Threshold X**"); or

    (b) Where the data breach is, or is likely to be, of a significant scale ("**Notification Threshold Y**"). Significant scale looks at how many individuals have been

back to top

impacted by the data breach. Where the number of individuals impacted by the data breach is 500 or more, it is deemed to be of significant scale.

(Notification Threshold X and Notification Threshold Y shall be collectively referred to as the "**Notification Thresholds**")

13. Notification Threshold X does not look at the number of individuals affected by the data breach. It focuses on the nature of the personal data that has been the subject of the data breach. The fact that there is only 1 individual affected by the data breach is sufficient to trigger Notification Threshold X if the nature of the personal data impacted falls within the Notification Threshold X formula of significant harm. The Personal Data Protection (Notification of Data Breaches) Regulations 2021 provides for a list of situations as to which significant harm is deemed to have occurred. It is important to bear in mind that this list is non-exhaustive. Hence, despite the following not being mentioned in the said list, this author would posit that the mere compromise of an individual's identification number (such as his/her NRIC number) alone would suffice to trigger Notification Threshold X.

14. Notification Threshold Y casts the net wide in capturing data breaches that arguably cause no or little harm to an affected individual. This is because the focus of Notification Threshold Y is the number of individuals affected and not the nature of the personal data that has been compromised. Various other jurisdiction(s)' mandatory data breach notification regimes are triggered only where there has been or there is likely to be harm caused to the affected individual. Notification Threshold Y means that a data breach which may not be notifiable under another jurisdiction's mandatory data breach notification regime, would be captured by the PDPA's mandatory data breach notification regime. This triggering difference is one of the reasons why the Singapore subsidiary of a multinational conglomerate must not simply adopt the data breach management plan or policy that it has issued for its European entities but instead require a standalone or supplementary data breach management plan to deal with the PDPA.

15. Many data breaches can therefore trigger Notification Threshold Y, so long as the number of individuals affected is at least 500. As an example, a simple list headlined as VIP members of a consumer facing company, who are attending the company's cocktail event on a specific date with 600 individuals listed, comprising their full names and the type of membership tier each member has, such as Gold, Silver or Black (assuming there are these 3 membership tiers) could trigger Notification Threshold Y if such list was inadvertently disclosed or lost.

D. Timelines

16. There are two spheres of timelines that an organisation needs to implement operationally. The first is when it is established that a data incident is a 'data breach' as defined in the PDPA. The second is after it has been established that the data breach meets one of the two Notification Thresholds.

back to top

17. Let us consider the first timeline. Where the organisation has reason to believe that a data breach affecting personal data in the organisation's possession or control has occurred, the organisation must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach meets any of the Notification Thresholds, and the PDPC has taken the position that this assessment should not exceed 30 calendar days[5].

18. This does not mean that an organisation can take its time to wait out the full 30 calendar days to deal with the triggering of one or both of the Notification Thresholds. Should it establish at an early stage (shorter than the 30 calendars) that indeed one of the Notification Thresholds has been met, that would mean that the next timeline of dealing with a triggered Notification Threshold would kick in.

19. Let us consider the second timeline. Once it has been established that one of the Notification Thresholds is met, the affected organisation has to notify the PDPC of the data breach within 3 calendar days. In the case where the data breach has triggered Notification Threshold X, the organisation has to additionally notify the affected individuals. The timeline for doing so is "*on or after*" notifying the PDPC.

20. It is pertinent to note that the PDPA provides for 2 exceptions whereby even though Notification Threshold X has been triggered and the organisation needs to notify both the PDPC and the affected individuals, there is no need for the organisation to notify the affected individuals[6]. The 2nd exception is subject to debate. It provides that there is no need to notify the affected individual if the organisation :

> "*had implemented, prior to the occurrence of the notifiable data breach, any technological measure that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual.*"

One cannot but contend that if indeed the organisation had prior to the occurrence of the data breach falling within Notification Threshold X, implemented a technological measure that prevents significant harm to the affected individual, then surely Notification Threshold X would not have been met and hence not triggered; and in such a case, there would not even be a need to notify the affected individual.

E. Operationally dealing with a data breach

21. From the foregoing, it should be clear to an organisation that navigating statutory requirements of a mandatory data breach notification regime, whether of Singapore or any other country's, is not a 'walk in the park'. When a data incident occurs, the organisation would need to deal with many substantive issues including but not limited to determining whether the data incident is considered a data

[5] Advisory Guidelines on Key Concepts in the Personal Data Protection Act
[6] Section 26D(5) of the PDPA.

back to top

breach under the PDPA, dealing with the statutory timelines of handling the data breach, assessing whether the data breach meets one of the Notification Thresholds, and reporting it to the PDPC. It is therefore in the interest of the organisation to seek external assistance from specialist lawyer(s) with expertise on dealing with a data breach, to handhold the organisation in meeting its statutory requirements. In fact, it may be the case that the specialist lawyer could very well assess that the data breach does not meet a Notification Threshold, thus obviating the statutory need to notify the PDPC or affected individuals. The specialist lawyer could also commission a technical forensics specialist to investigate the cause of the data breach in order to obtain key facts of the types of personal data and number of individuals, involved in the data breach. By involving the specialist lawyer to commission the technical forensics specialist, the report from the technical forensics specialist procured by the specialist lawyer could be endowed with legal privilege; a benefit that an organisation would not be able to obtain if engaging the technical forensics specialist directly.

F. Conclusion

22. This article has been written with the objective of providing a brief overview of the subject in question, and does not purport to cover all the issues and requirements under the PDPA's mandatory data breach notification regime.

23. The contents of this article does not constitute legal advice - In particular, each data incident has its own peculiarities and specificities and upon a data incident happening, the organisation should immediately seek legal advice on it.

About Rajah & Tann Cybersecurity
Rajah & Tann Cybersecurity, member of Rajah & Tann Technologies Group, is uniquely placed to help clients protect, mitigate against attacks, minimise disruptions from a security breach and effectively deal with a data breach. Email us at info@rtcyber.com for enquiry.

Article from Cyber Threat Intelligence SIG

Rantings of a Cyber Security Analyst

Layered Defense. I am sure many in the security field has heard this term. Most understand this as having different solutions to protect different portions of the infrastructure. A firewall for networking, endpoint protection for the devices, some form of Multi Factor Authentication for better verification of access… the list goes on.

What I personally feel goes wrong is treating this as a checklist. Do I have a firewall? Check. Endpoint Security? Check. Once all these requirements are checked, my security is good. Right?

back to top

