
# Regulations at a Glance for Financial Institutions:

# Reconciling the Draft Cybersecurity Bill, the Monetary Authority of Singapore Regulations and the Public Consultation for Approaches to Managing Personal Data in the Digital Economy

**A Report by OC Queen Street LLC,**

**Osborne Clarke's associated Singapore Law Practice**

## TABLE OF CONTENTS

## PART I: OVERVIEW

### 1. Executive Summary

1.1 We refer to the following documents:

a. "Public Consultation for Approaches to Managing Personal Data In the Digital Economy" ("**Consultation Paper**")[1] which was issued by the Personal Data Protection Commission Singapore ("**PDPC**") on 27 July 2017;

b. "Draft Cybersecurity Bill" ("**Draft Bill**")[2] which was issued by the Ministry of Communications and Information ("**MCI**") and the Cyber Security Agency of Singapore ("**CSA**") on 10 July 2017;

c. "Notice 644 on Technology Risk Management" ("**TRM Notice 644**")[3] and "Notice CMG-N02 on Technology Risk Management" ("**TRM Notice CMG-N02**")[4] (collectively, the "**TRM Notices**") which were issued by the Monetary Authority of Singapore ("**MAS**") on 21 June 2013.

1.2 Personal data protection has become an increasingly important and unavoidable concept with the advent of the digital economy, which brings with it the emergence of Internet of Things devices, big data and artificial intelligence. These new technological developments have resulted in a shift from active to passive data collection, where the sheer volume of collection, usage and disclosure of personal data necessitates the development of new regulations to govern its processing.

1.3 In this submission, we will address the need for consent as a basis for processing personal data, the situations in which other bases may be more appropriate and the need to benchmark our consent requirements to facilitate the data transfer obligations of other jurisdictions.

1.4 In addition, we will also discuss the proposed introduction of mandatory data breach notifications in the Consultation Paper and the approaches other jurisdictions apply in the event of data breaches.

1.5 Lastly, we will propose the possible harmonisation of the Consultation Paper, Draft Bill and TRM Notices in order to reduce the regulatory burden on financial institutions (the "**FIs**"). The TRM Notices and the Draft Bill regulate many similar aspects of data breaches. Thus, we suggest that FIs be exempted from the Draft Bill insofar as it overlaps with the TRM Notices.

1.6 In this respect, we recommend:

(a) Collaborative reporting between FIs and MAS, CSA and PDPC (collectively, the "**regulatory agencies**"), where notifying MAS and/or PDPC in the event of a data breach will suffice.

(b) Collaborative investigating between FIs and the regulatory agencies, where only MAS and/or PDPC will investigate should the need arise.

(c) Greater coordination between the regulatory agencies.

[1] Public Consultation for Approaches to Managing Personal Data In the Digital Economy, issued 27 July 2017
[2] Draft Cybersecurity Bill, issued 10 July 2017
[3] Monetary Authority of Singapore Notice 644 on Technology Risk Management, issued on 21 June 2013
[4] Monetary Authority of Singapore Notice CMG-N02 on Technology Risk Management, issued on 21 June 2013

1.7 Prior to this submission, we hosted a roundtable with in-house lawyers from 15 different corporations across the financial services, information services and telecommunications industries to obtain their views on the proposed amendments to the Personal Data Protection Act (the "**PDPA**")[5] in the Consultation Paper and our proposed harmonisation of the Consultation Paper, Draft Bill and the TRM Notices.

1.8 Their feedback, together with some of our views, have since been collated into this document, which will serve as our response to the Consultation Paper. Notwithstanding, the comments found in this submission are attributable only to OC Queen Street LLC and not the participants who may have provided comments.[6]

## 2. Definition and scope of the definition of "personal data": What constitutes personal data?

2.1 Section 2(1) of the PDPA defines "personal data" as follows:

> *"personal data" means data, whether true or not, about an individual who can be identified —*
> *(a) from that data; or*
> *(b) from that data and other information to which the organisation has or is likely to have access*

2.2 This definition of personal data appears to be used across more than merely the PDPA regulatory framework. The MAS Notices on Prevention of Money Laundering and Countering the Financing of Terrorism (collectively, the "**AML/CFT Notices**")[7] specify that personal data in those notices is has the same meaning as defined in Section 2(1) of the PDPA.

2.3 In addition, this definition of personal data also appears to cohere with how personal information is defined in the Computer Misuse and Cybersecurity Act (the "**CMCA**")[8] at Section 8A(7)(a), where:

> *personal information is any information, whether true or not, about an individual of a type that is commonly used alone or in combination with other information to identify or purport to identify an individual, including (but not limited to) biometric data, name, address, date of birth, national registration identity card number, passport number, a written, electronic or digital signature, user authentication code, credit card or debit card number, and password.*

2.4 The concept of personal data was also discussed at the roundtable, where it was suggested that personal data is often a subset of customer information. As such, the concept of personal data is pertinent to FIs, given that they are governed by sectoral regulations from the MAS, as well as statutory regulations such as the Securities and Futures Act (the "**SFA**")[9] and the Banking Act (the "**BA**").[10]

---

[5] Personal Data Protection Act, Singapore.
[6] This report was prepared with time constraint and thus does not purport to be comprehensive, but merely points out some of the issues that may warrant further consideration.
[7] Various AML/CFT Notices apply to different FIs, such as the MAS Notice 626 Notice on Prevention of Money Laundering and Countering the Financing of Terrorism (Banks) which applies to all commercial banks in Singapore.
[8] Computer Misuse and Cybersecurity Act, Singapore.
[9] Securities and Futures Act, Singapore.
[10] Banking Act, Singapore.

2.5 Indeed, the MAS Guidelines on Outsourcing[11] mainly defines customer information as:

(i) "user information" as defined in Section 2(1) of the SFA; or

(ii) in general, information that relates to its customers and these include customers' accounts, particulars, transaction details and dealings with the financial institutions, but does not include any information that is public, anonymised, or encrypted in a secure manner such that the identities of the customers cannot be readily inferred.

2.6 In turn, Section 2(1) of the SFA defines user information to be as follows:

*"user information" means transaction information that is referable to —*

*(a) a named user; or*

*(b) a group of users, from which the name of a user can be directly inferred*

2.7 Likewise, the Section 40A of the BA defines customer information to be as follows:

*"customer information", in relation to a bank, means —*

*(a) any information relating to, or any particulars of, an account of a customer of the bank, whether the account is in respect of a loan, investment or any other type of transaction, but does not include any information that is not referable to any named customer or group of named customers; or*

*(b) deposit information;*

*"deposit information", in relation to a bank, means any information relating to —*

*(a) any deposit of a customer of the bank;*

*(b) funds of a customer under management by the bank; or*

*(c) any safe deposit box maintained by, or any safe custody arrangements made by, a customer with the bank,*

*but does not include any information that is not referable to any named person or group of named persons;*

2.8 Even across international jurisdictions, the concept of personal data appears to be largely universal. Article 4(1) of the recently approved General Data Protection Regulation (the "**GDPR**")[12] of the European Union (the "**EU**") defines personal data as:

*...any information relating to an identified or identifiable natural person ('data subject');*

[11] MAS Guidelines on Outsourcing, issued 27 July 2016.
[12] General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679), issued on 27 April 2016.

*an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*

this definition was utilised in the United Kingdom's (the "**UK**") Information Commissioner's Office (the "**ICO**") Consultation on the GDPR Consent Guidance.

2.9 All of these definitions, despite differing slightly in structure, all include the capacity for identification of a specific individual. Thus, it appears that personal data, in general, encompasses any data or information from which an identity of an individual can be identified or inferred.

## 3. Comparison between different "data protection" regimes

3.1 Currently, there exists a number of key "data protection" regimes in Singapore that govern and regulate different entities with regards to the processing of information. Such information regulation regimes include the TRM Notices, the Draft Bill, the PDPA and the CMCA.

3.2 The table below sets out the aforementioned key "data protection" regimes.

| | **TRM Notices** | **Draft Bill** | **PDPA** | **CMCA** |
|---|---|---|---|---|
| **Regulatory Authority** | MAS | CSA / Commissioner of Cybersecurity ("**Commissioner**") | PDPC | Ministry of Home Affairs ("**MHA**") |
| **Year Introduced** | 2013 | 2017 | 2012 | 1993 |
| **Parties Affected / Responsible** | FIs | Owners of Critical Information Infrastructure ("**CIIOs**") | All organisations except:<br>(a) Individuals acting in a personal/domestic capacity;<br>(b) Employee acting in the course of his employment;<br>(c) Public agency (or organisation acting on behalf of); and<br>(d) Data intermediaries | All individuals regardless of nationality or citizenship outside or within Singapore |
| **Types of Information Regulated** | Customer Information | Critical Information Infrastructure ("**CII**")[13] | Personal Data | Personal Information |

Table 1: Comparison of parties and information regulated under key "data protection" regimes

[13] Section 2(1) Draft Cybersecurity Bill: "critical information infrastructure" means a computer or a computer system that is necessary for the continuous delivery of essential services which Singapore relies on, the loss or compromise of which will lead to a debilitating impact on the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore.

3.3 The CMCA was first introduced in 1993 as an Act to make provision for securing computer material against unauthorised access or modification, to require or authorise the taking of measures to ensure cybersecurity. While Section 15A of the CMCA provides some existing powers related to cybersecurity, these will be enhanced by the Cybersecurity Bill with specific powers vested in CSA officers.

3.4 As can be seen, there has been a shift towards increased data protection in recent years. The PDPA was first introduced in 2012 to govern the collection, use and disclosure of personal data by organisations, and to establish the Do Not Call Register and to provide for its administration. The PDPA is currently undergoing review, which forms the basis of this submission to critique the recommendations by the PDPC and to offer alternative suggestions where necessary.

3.5 In 2013, the TRM Notices and their accompanying Technology Risk Management Guidelines ( the "**TRM Guidelines**")[14] were introduced for the purpose of establishing a robust technology risk management framework to protect customer information, transactions and systems. The TRM Guidelines and TRM Notices were issued by MAS, and were part of the sectoral regulations that governed the FIs.

3.6 Following an increasingly worrying trend of cybersecurity incidents such as the Advanced Persistent Threat (the "**APT**") attacks suffered by the National University of Singapore and Nanyang Technological University, and the WannaCry ransomware attacks on digital signage provider MediaOnline, the Draft Bill was introduced in 2017.

3.7 The Draft Bill aims to establish a framework for the regulation of CIIOs, to provide CSA with powers to manage and respond to cybersecurity threats, to establish a framework for the sharing of cybersecurity information, and to introduce a lighter-touch licensing framework for the regulation of selected cybersecurity service providers.

3.8 The CMCA was further amended in April 2017 to criminalise dealing in personal information obtained via a cybercrime,[15] as well as dealing in hacking tools to commit a computer offence.[16]

3.9 It is also now an offence under the CMCA for someone committing a criminal act while overseas, against a computer located overseas, should the act "cause or create a significant risk of serious harm in Singapore".[17] Presumably, this is in response to a surge in global cybercrime such as ransomware, banking fraud and disruptions to Internet services – all of which can be committed remotely from a computer outside Singapore.

3.10 Hence, it can be seen that these four key data protection regimes have different purposes. While both the CMCA and the Draft Bill govern cybersecurity in Singapore, the former has a largely punitive function, whereas the latter serves as a regulatory framework for CII. In a similar vein, while both the PDPA and the TRM Notices protect personal information, the PDPA creates a general framework protecting personal data, whereas the TRM Notices carry more sector-specific obligations that regulate FIs.

[14] MAS Technology Risk Management Guidelines, issued June 2013.
[15] Section 8A CMCA.
[16] Section 8B CMCA.
[17] Section 11 CMCA.

3.11 Nonetheless, it is evident that FIs may be caught under the provisions of the TRM Notices, the Draft Bill and the PDPA should they experience a data breach as it appears that the Draft Bill and the TRM Notices regulate similar FIs.

3.12 The First Schedule in the Draft Bill specifies the following services relating to banking and finances as essential services that are likely to be classified as CII:

(a) Retail and commercial banking services;
(b) Payments clearing and settlement services;
(c) Securities trading, clearing, settlement and depository services;
(d) Derivatives trading, clearing and settlement services;
(e) Monetary management operations (MMO) and intervention operations (IO) services;
(f) Services related to mobilisation of official foreign reserves (OFR);
(g) Currency issuance;
(h) Services related to cash management and payments for the Government.

3.13 Section 1 of both the TRM Notices specify that they apply to all:

(i) banks;
(ii) approved exchanges;
(iii) licensed trade repositories;
(iv) approved clearing houses;
(v) recognised clearing houses which are incorporated in Singapore;
(vi) holders of a capital markets services licence;
(vii) recognised market operators which are incorporated in Singapore; and
(viii) persons who are approved under Section 289 of the SFA to act as a trustee of a collective investment scheme which is authorised under section 286 of the SFA and constituted as a unit trust.

3.14 Furthermore, all private organisations are required to comply with the PDPA.

3.15 Thus, whether FIs should be subject to reporting and investigatory obligations from MAS, CSA and PDPC remain a subject of debate.

## PART II: CONSENT

### 4. Strengthening Consent as a Legal Base

4.1 In addition to moving towards a system of parallel bases for the collection, use and disclosure of personal data, it is important that Singapore also strengthens the regulations for consent. This is to ensure that Singapore meets the data protection standards of other jurisdictions such as the EU.

4.2 Under the GDPR, consent is one of six legal bases for the processing of personal data.[18] The GDPR's predecessor, EU Directive 95/46/EC, treated all data processing as prima facie illegitimate. Data processing would only be legitimized if it fell under one of the six legal grounds.[19] This approach has been carried forward in the GDPR, which treats processing as unlawful unless it falls under one of the six legal bases.[20] Although consent from the data subject has the effect of legitimizing personal data processing operations,[21] it should not be considered the primary ground for the processing of personal data.[22]

4.3 Where consent is required, controllers must be able to demonstrate that the data subject consented to the processing of his/her data.[23] Consent must be in the form of a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him/her.[24]

4.4 This indication must be made in the form of a statement or by clear affirmative action.[25] This requires an active opt-in mechanism, such that silence, pre-ticked boxes or default settings will not suffice. Example opt-in mechanisms provided by the ICO include:[26]

(1) Signing a consent statement on a paper form
(2) Ticking an opt-in box on paper or electronically
(3) Selecting from equally prominent yes/no options
(4) Responding to an email requesting consent
(5) Answering yes to a clear oral consent request

4.5 The request for consent must specifically include the controller's name, the purposes of the processing and the types of processing activity.[27] Whether consent was freely given will depend on whether the performance of a contract is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.[28] As such, if the data subject has no genuine or free choice, or is unable to refuse or withdraw consent without detriment, consent will not be regarded as given freely.[29]

---

[18] GDPR Article 6(1)
[19] EU Directive 95/46/EC, Section II
[20] GDPR Article 6
[21] Article 29 Working Party, "Opinion 15/2011 on the definition of consent", at II.1.
[22] Article 29 Working Party, "Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of the Directive 95/46/EC", at III.2.1.
[23] GDPR Article 7(1)
[24] GDPR Article 4(11)
[25] *ibid.*
[26] Information Commissioner's Office, "Consultation: GDPR Consent Guidance", at pg 31-32
[27] *ibid.* at pg 18
[28] GDPR Article 7(4)
[29] GDPR Proviso 43

4.6 If consent is given as a written declaration which also concerns other matters, the request for consent must be presented:[30]

(a) In a manner which is clearly distinguishable from other matters, kept separate from other terms and conditions
(b) In an intelligible and easily accessible form
(c) Using clear and plain language

A data subject will not be bound by a written declaration if the above conditions are not met.

4.7 Proof that consent was obtained must be recorded by the controller.[31] If data processing was done subject to the data subject's consent, the data subject has the right to data portability.[32] The data subject also has the right to withdraw his/her consent at any time, and withdrawing consent must be as easy to do as giving consent.[33] If consent is withdrawn, the data subject has the right to erasure (also known as the right to be forgotten).[34]

4.8 Using consent as a legal basis for processing will give consumers real choice and control over how their data is used. Further, consent may improve the level of engagement between organization and consumer, encouraging consumers to trust organisations with more useful data.[35]

4.9 Consent may nonetheless be an inappropriate legal base in certain circumstances. For example, if you would process the data on a different lawful basis if consent is refused, if you are asking for consent as a precondition of accessing services, or if you are in a position of power over the data subject.[36]

4.10 A higher standard of regulation is imposed on the processing of special categories of personal data. This refers to:[37]

(a) Data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership
(b) Genetic data
(c) Biometric data for the purpose of uniquely identifying a natural person
(d) Data concerning health
(e) Data concerning a natural person's sex life or sexual orientation

## 5. Parallel Bases for Collecting, Using and Disclosing Personal Data in the EU

5.1 Under the GDPR, there are six legal bases under which data processing is lawful:[38]

(1) The data subject consented to the processing of his/her data for one or more specific purposes;

[30] GDPR Article 7(2)
[31] GDPR Article 7(1)
[32] GDPR Article 20
[33] GDPR Article 7(3)
[34] GDPR Article 17
[35] Information Commissioner's Office, "Consultation: GDPR Consent Guidance", pg 12
[36] *ibid.* at pg 13
[37] GDPR Article 9(1)
[38] GDPR Article 6(1)

(2) Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(3) Processing is necessary for compliance with a legal obligation to which the controller is subject;
(4) Processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(5) Processing is necessary for the performance of a public task;
(6) Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

These legal bases have been carried forward from Directive 95/46/EC of the European Union, in the context of which the Article 29 Working Party has provided guidance.[39]

**Article 6(1)(b): Processing necessary for the performance of a contract**

5.2 This provision must be interpreted strictly, and does not cover situations where the processing is not genuinely necessary for the performance of the contract.[40] For example, if the contract was for the delivery of goods and services from an online portal, building a profile of a user's tastes and lifestyle choices from his actions on the website will not be considered necessary for the performance of the contract.[41] Processing triggered by non-compliance with a contract, or to all other incidents in the execution of a contract will not be covered by this base.[42]

**Article 6(1)(c): Processing necessary for compliance with a legal obligation**

5.3 The processing must have a basis in EU or State law, although not any law specifically.[43] This might be the case where employers are required to report salary data to tax authorities, or where financial institutions are obliged to report certain suspicious transactions under anti-money-laundering rules.[44] This also only refers to a legal obligation derived from the laws of the EU or a member state, and legal obligations of third countries are not covered under Article 6(1)(c).[45]

**Article 6(1)(d): Processing necessary to protect the vital interests of the data subject or another person**

5.4 This legal ground is intended to protect an interest which is essential to the data subject's life,[46] and is applicable in situations where there is a threat posing a risk of injury or other damage to the health of the data subject.[47] There is nonetheless some uncertainty as to whether the threat must be immediate.[48] The WP further suggests that in situations where there is a possibility and

[39] Article 29 Working Party, "Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC"
[40] *ibid.* at III.2.2.(i)
[41] *ibid.*
[42] *ibid.*
[43] GDPR Recital 45
[44] Article 29 Working Party, "Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", at III.2.3.
[45] *ibid.*
[46] EU Directive 95/46/EC, Proviso 31
[47] Article 29 Working Party, "Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", at III.2.4.
[48] *ibid.*

need to request valid consent, consent should be sought.[49] This would further limit the application of Article 6(1)(d) to a case-by-case analysis, rather than to legitimize any massive collection or processing of personal data.[50]

**Article 6(1)(e): Processing for the purpose of a public task**

5.5 The ICO suggests that processing necessary for the performance of a public task will likely provide a legal basis for most activities by a public authority.[51] Nonetheless, the element of necessity must still be proven; that the processing is necessary to carry out your functions, and that it is proportionate and there is no less intrusive alternative.[52] The general principle that data processing must be fair, transparent and accountable must also be taken into account. Further, if the public authority is acting for purposes other than its official functions, processing in this regard will not be necessary for the performance of a public task. It should be noted that Singapore already exempts public agencies or organisations from data processing regulations.[53]

**Article 6(1)(f): Processing for a legitimate interest**

5.6 A legitimate interest can include a commercial benefit, however this interest must not be outweighed by harm to the individual's rights and interests.[54] This "legitimate interests" exception has been carried forward from the UK Data Protection Act,[55] in the context of which the ICO provided guidance. For the legitimate interest condition to be met, the organization must:[56]

(1) Need to process the information for the purposes of your legitimate interests, or for those of a third party to whom you disclose it.
(2) These interests must be balanced against the interests of the individuals concerned. If the processing is unwarranted due to its prejudicial effect on the rights and freedoms, or legitimate interests, of the individual. While your legitimate interests do not need to be in harmony with those of the individual in question, the individual's legitimate interests will take precedence in the event of a serious mismatch.
(3) The processing of information under the legitimate interests condition must be fair, lawful and comply with all the data protection principles.

5.7 Further guidance is provided by the WP. The interest in question must be a real and present interest, corresponding with current activities or benefits that are expected in the very near future. Vague or speculative interests will be insufficient.[57]

5.8 Even if the controller's interest is legitimate, if the interest fails the following balancing test this base cannot be relied on.[58] This is not a straightforward balancing test, and is instead a

[49] Article 29 Working Party, "Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", at III.2.4.
[50] *ibid.*
[51] Information Commissioner's Office, "Consultation: GDPR Consent Guidance", pg 16
[52] *ibid.*
[53] Personal Data Protection Act 2012 (Singapore), Section 4(1)(c)
[54] Information Commissioner's Office, "Consultation: GDPR Consent Guidance", pg 16
[55] The UK government on 14 September 2017 has published the first draft of its proposed new Data Protection Bill in support of GDPR in the UK. This bill has not been considered in the preparation of this report.
[56] Information Commissioner's Office, "The conditions for processing", found at <https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/>
[57] Article 29 Working Party, "Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", at III.3.1.
[58] *ibid.*

complex assessment taking into account a number of factors.[59] For example, the WP acknowledged that a company had a legitimate interest in complying with subpoenas under US law, such as to avoid the risk of US sanctions.[60] Nonetheless, the company conducted the processing of data in a hidden, systematic, massive and long-term manner, without having specified the further incompatible purpose at the time of processing. The company further did not point this purpose out to the users of its service. Given the far-reaching effects this processing could have on any individual, the WP considered that the interests for fundamental rights and freedoms of the numerous data subjects overrode the company's interest not to be sanctioned by the US.[61]

5.9 The WP also suggested that if the interest pursued by the controller is not compelling, the interests and rights of the data subject are more likely to override the legitimate, but less significant – interests of the controller. Nonetheless, if there is a reduced impact of processing on data subjects, less compelling interests of the controller may still override their interest.[62]

5.10 In actually applying the balancing test, the WP provides four factors to be taken into consideration:[63]

(1) Assessing the controller's legitimate interest, including for the exercise of a fundamental right or for the interests of the wider community
(2) The impact on the data subjects
(3) Provisional balance
(4) Additional safeguards applied by the controller to prevent undue impact on the data subjects

## 6. Proposed 'notification of purpose' base

6.1 Many jurisdictions require the organisation processing personal data to notify a supervisory authority, upon which the latter will publish a public register for individuals to consult. Such countries include the United Kingdom, which requires organisations to inform the Information Commissioner's Office.[64]

6.2 However, other key jurisdictions, such as Australia, have adopted a regime similar to the one proposed. Australia's Privacy Act 1988 largely allows organisations to notify individuals in lieu of obtaining consent, as long as the notification covers issues such as purposes of collection and consequences if personal information is collected, among others.[65]

6.3 Such an approach will allow organisations to function more effectively and efficiently, especially if the collection, usage and disclosure of personal data is for the purposes of enhancing consumer experience. For example, where an organisation lacks its customers' contact information but aims to analyse their personal data to improve their product offering.

---

[59] Article 29 Working Party, "Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", at III.3.1.
[60] Article 29 Working Party, "Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (Swift)", at 4.2.3
[61] *ibid.*
[62] Article 29 Working Party, "Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC", at III.3.4
[63] *ibid.*
[64] Data Protection Act 1988 (United Kingdom), Section 18
[65] Privacy Act 1988 (Australia), Schedule 1, Part 2 The Australia Privacy Act 1988 also appears to generally require organisations to collect personal information directly from the individual concerned.

6.4 In order to prevent organisations from collecting, using or disclosing personal data indiscriminately, the proposed Notification of Purpose approach should be limited to circumstances where it is impractical to obtain consent and when an individual's rights are not prejudiced.

6.5 The GDPR stipulates to take special care with personal data that reveals sensitive information that puts the rights and freedoms of individuals at risk, such as personal data that reveals racial or ethnic origin, political opinions, religion or philosophical beliefs, biometric data and sexual orientation among others.[66]

6.6 Likewise, the UK's Data Protection Act 1998 requires organisations processing sensitive personal data including racial or ethnic origin, political opinions or religious beliefs, among others, to obtain explicit consent from the affected individuals.[67]

6.7 Further to this, information and communication relating to the collection, processing and usage of personal data should be transparent, in line with the GDPR.[68] This includes informing individuals of the purposes of collecting their personal data, and should be further reinforced by measures to assess and mitigate risks such as a data protection impact assessment, encrypting personal data obtained and ensuring vendors comply with similar strict security standards.

## 7. Proposed 'legal or business purpose' base

7.1 The scope of the "legal or business purpose" base requires further clarification. During the roundtable, participants expressed concern over the scope of the "legal or business purpose" base, suggesting that its broad definition rendered it susceptible to abuse. Further, it was pointed out that from a business perspective, it was difficult to envisage a purpose which was not a business purpose. Conversely, participants noted that due to the ambiguous nature of the definition, relying on the mechanism could present an operational risk arising from the possibility of accidental non-compliance.

7.2 As this base shares similarities with several of the EU's legal bases, it is proposed that the "legal or business purpose" base is redefined as "necessary for the performance of a contract", "necessary for compliance with a legal obligation" and "necessary for a legitimate interest" bases. This would be assistive to commercial certainty.

7.3 Regardless of implementation, individuals should still be notified if an organization is collecting, using or disclosing personal data without their consent. This is comparable to the GDPR, which states that individuals should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data, and how to exercise their rights in relation to such processing.[69] Even though the individual may not withdraw consent, notification is still meaningful in enabling individuals to exercise informed choice regarding their use and choice of service providers. Similarly, the GDPR provides for individuals to object to any processing undertaken pursuant to "legitimate interests", which is the clause that the 'legal or business

[66] GDPR Article 9
[67] Data Protection Act 1988 (United Kingdom), Schedule 3
[68] GDPR Article 12
[69] GDPR, Recital 39

purpose' mechanism stems from. Once an objection has been raised, the organisation should provide "compelling legitimate interest" grounds for the deployment of this mechanism.[70]

## 8. Implications for Singapore's data processing requirements

8.1 The move to a system of parallel bases for the collection, use or disclosure of personal data is welcome. Nonetheless, it is important that the consent base is strengthened alongside the introduction of the "notification of purpose" and "legal or business purpose bases. This is to ensure that Singapore's standard of data protection meets the requirements of other jurisdictions such as the EU and Australia.

8.2 With the increased transfer of data across borders and jurisdictions as a result of a greater reliance on online IT services, cloud-based services, remote access services or global HR databases, there is a need to ensure that Singapore's requirements on the processing of personal data are aligned to those of other jurisdictions. This is because many jurisdictions only permit data transmission if an adequate level of data protection is ensured in the country of the recipient.

8.3 In the absence of an adequate level of data protection, organisations may have to rely on a consent exemption or employ more stringent data privacy safeguards which may result in increased time costs. Moreover, it may also result in a decrease in Singapore's viability as a data processing or cloud computing hub.

8.4 For example, the EU imposes stringent controls on transferring personal data outside the EU. The GDPR provides that transfers of personal data to a country outside the EU or an international organization may take place where the European Commission has decided the country or organization in question ensures an adequate level of protection,[71] or if the controller has provided adequate safeguards and enforceable data subject rights and remedies are available.[72] In the absence of an adequacy decision or appropriate safeguards, controllers can still transfer data in the following situations:[73]

(1) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
(2) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
(3) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
(4) The transfer is necessary for important reasons of public interest;
(5) The transfer is necessary for the establishment, exercise or defence of legal claims;
(6) The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
(7) The transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down in Union or Member State law for consultation are fulfilled in the particular case.

[70] Recital 69 read together with Article 6(1)(f), Article 13(1)(a) and Article 14(2)(e), GDPR, European Union.
[71] GDPR Article 45(1)
[72] GDPR Article 46(1)
[73] GDPR Article 49(1)

(8) The transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

The first three exceptions are however not applicable in the case of activities carried out by public authorities in the exercise of their public powers.[74]

8.5 Similarly, the Australian Privacy Act 1988 provides that organisations must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles in the Privacy Act 1988 should they disclose personal data to an overseas recipient.[75] In certain circumstances, an organisation can be held liable when it discloses personal data overseas and the overseas recipient breaches the APPs in relation to that data. However, the requirement does not apply if the organization obtains the informed consent of the relevant data subjects as stipulated. Nonetheless, informed consent is difficult to obtain as organisations have to ascertain that individuals have read the applicable privacy policy.

[74] GDPR Article 49(3)
[75] Privacy Act 1998 (Australia), Schedule 1, Privacy Principle 8

## PART III: MANDATORY DATA BREACH NOTIFICATIONS

### 4. Threshold of notification too low: Imposition of onerous regulatory burdens

9.1 The proposed criteria for data breach notification may be too cumbersome and onerous as it appears to protect the interests of affected individuals via strict regulatory requirements at the expense of businesses. For example, the threshold for notification, being that of "any risk of impact of harm", is set much lower than other jurisdictions.

9.2 In comparison, Australia uses the threshold test of a "reasonable person" concluding that the breach is "likely to result in serious harm" in the Privacy Amendment (Notifiable Data Breaches) Act 2017.[76] Similarly, in the EU's GDPR approved in April 2016, individuals only have to be informed when there is a high risk to their rights and freedoms.[77]

9.3 Furthermore, there is no single federal statute in the United States that makes breach notification mandatory, and instead individual states have varying data breach notification laws that apply mostly only to particularly sensitive enumerated types of data such as Social Security Numbers or driver's license numbers.[78]

9.4 On the other hand, the proposed criteria for a significant scale of breach appears to be in line with breach notification regulations of various jurisdictions. For example, California, Florida, Iowa, Rhode Island and Washington all require organisations to inform either the state Attorney-General's office or the state Department of Legal Affairs of data breach notifications involving more than 500 state residents.[79]

### 5. Exemption of public bodies from breach notification requirements lacks justification

10.1 The proposed exclusions from breach notification under Section 4 of the PDPA applying to individuals and organisations such as public agencies, among others, do not mirror that of different jurisdictions around the world. For example, only 11 states in the USA, including Colorado, Maine and Vermont, do not require government agencies to comply with data breach notification regulations.[80]

10.2 Indeed, California, which the PDPC references in its draft review of the PDPA, requires state agencies to comply with such regulations as well.[81] Furthermore, the EU's GDPR makes no distinction between public and private bodies, and in fact makes the designation of a data protection officer mandatory where data processing is carried out by a public body.[82]

### 6. Exploring redaction as a possible safe harbor exception

11.1 The PDPC has also proposed similar safe harbour exceptions and law-enforcement exceptions adopted by various data protection regimes around the world. Encryption of data generally

[76] Section 26WE(2)(a)(ii), Division 2, Privacy Amendment (Notifiable Data Breaches) Act 2017, Australia.
[77] Article 34(1), GDPR, European Union.
[78] http://www.dwt.com/files/Uploads/Documents/Publications/State%20Statuets/BreachNoticeSummaries.pdf
[79] Ibid.
[80] Ibid.
[81] Ibid.
[82] Article 37(1), GDPR, European Union.

provides an exemption to disclosure requirements in the 47 states in the USA which have data breach notification regulations.[83]

11.2 However, some states have also provided for exemptions from breach notification where personal data was redacted but not encrypted. For example, 21 states in the USA, including Pennsylvania, Michigan, Ohio and Vermont, have safe harbour exceptions which extend to redacted information which was disclosed.[84]

11.3 The Canadian Internet Policy and Public Interest Clinic (CIPPIC) proposal for a Canadian data breach notification law also proposes exceptions for 'information that is redacted or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable by unauthorized persons'.[85]

11.4 This could similarly be considered by the PDPC for disclosed information which is not determined to pose a risk of harm to affected individuals.

## 7. Time frames for breach notifications not unduly stringent

12.1 The PDPC's proposed time frames for data breach notifications to the PDPC is commensurate with or more stringent than other key jurisdictions such as EU, Australia, and the USA. In fact, the threshold proposed by the PDPC is high than that of the EU, whose GDPR requires that data controllers notify the national data protection authority of a personal data breach within 72 hours of discovery unless the breach is "unlikely to result in a risk to the rights and freedoms of natural persons".[86]

12.2 In addition, Australia's Privacy Amendment (Notifiable Data Breaches) Act 2017 provides for a 30-day assessment period before the organisation is required to inform the Australian Privacy Commissioner.[87]

12.3 Similarly, its proposed time frames for data breach notifications to affected individuals appears to be equivalent to other key jurisdictions. The "as soon as practicable" requirement proposed by the PDPC mirrors that of most USA states, which require that the organisation notifies affected persons as expediently as possible or practicable, without unreasonable delay or both.[88]

## 8. Exploring a time limit for breach notifications to individuals

13.1 However, the introduction of a specific timing requirement for notice to individuals could also be considered. Florida requires organisations to notify individuals as expeditiously as practicable and without unreasonable delay but no later than 30 days after the determination of a breach, and Ohio and Wisconsin both require notification within 45 days from the determination of a breach. This will allow affected individuals to take timely remedial actions to mitigate exposure from the data breach.[89]

---

[83] http://www.dwt.com/files/Uploads/Documents/Publications/State%20Statuets/BreachNoticeSummaries.pdf
[84] Ibid.
[85] CIPPIC White Paper on Approaches to Security Breach Notification, Page 15.
[86] Article 33(1), GDPR, European Union.
[87] Section 26WH(2)(b), Privacy Amendment (Notifiable Data Breaches) Act 2017, Australia.
[88] http://www.dwt.com/files/Uploads/Documents/Publications/State%20Statuets/BreachNoticeSummaries.pdf
[89] Ibid.

13.2 Nonetheless, in view of the potential costs and effort involved, perhaps a time limit could only be implemented should there be a "high risk to the rights and freedoms" of affected individuals. If this measure is adopted, it will be more stringent than that of the GDPR, which only requires organisation to notify affected individuals of data breaches "without undue delay".[90]

[90] Article 33(1), GDPR, European Union.

## PART IV: REDUCING THE REGULATORY BURDEN ON FINANCIAL INSTITUTIONS

### 9. Comparing the applicability of the Draft Cybersecurity Bill, TRM Notices 644 and CMG-N02 and Consultation Paper to Financial Institutions

***Overview***

14.1 The following table sets out a summary of the thresholds and timelines for notification to the respective regulatory bodies in the event of incidents which fall under the regulatory purview of the Draft Bill, TRM Notices and the Consultation Paper.

| | TRM Notices | Draft Bill | Consultation Paper |
|---|---|---|---|
| **Types of Information Regulated** | Customer Information | CII | Personal Data |
| **Threshold for Notification** | "Relevant incident"[91] | "Any (significant) cybersecurity incident"[92] | Notifying PDPC and affected individuals:<br>"Any risk of impact or harm" |
| | | | Notifying PDPC:<br>Where the scale of the data breach is significant (i.e. more than 500 individuals) |
| **Timeline for Notification** | Notifying MAS:<br>1 hour[93] | Notifying CSA:<br>Not stipulated yet[94] | Notifying affected individuals:<br>As soon as practicable |
| | Root cause and impact analysis report: 14 days[95] | | Notifying PDPC:<br>72 hours |
| **Legal Status and Penalty for Non-Compliance** | Legally binding.<br><br>FIs which contravene MAS directions w/o reasonable excuse are liable under the Securities & Futures Act and Banking Act to fines depending on the type of FI. The most onerous fine is ≤ $150,000. For continuing offences, fines of $15,000/day or part thereof. | Legally binding.<br><br>Failure by CIIOs to comply with notification requirement: Fine ≤ $150,000 or imprisonment ≤ 2 years or both. | Legally binding, but no specific penalty proposed for breaching notification requirement.<br><br>Under s56 Personal Data Protection Act, general penalty for non-compliance of a fine ≤ $10,000 or imprisonment ≤ 3 years or both. For continuing offences, |

[91]Section 2, TRM Notices 644/CMG-N02: "Relevant incident" is defined as a system malfunction or IT security incident, which has a severe and widespread impact on the financial institution's operations or materially impacts the financial institution's service to its customers.
[92] Section 10(1) and Section 15(1), Draft Cybersecurity Bill, Singapore.
[93] Section 7, TRM Notices 644/CMG-N02.
[94] Section 15(1), Draft Cybersecurity Bill, Singapore.
[95] Section 8, TRM Notices 644/CMG-N02.

| | | | |
|---|---|---|---|
| | | | fine of ≤ $1,000/day or part thereof. |

Table 2: Thresholds and timelines for notification and legal status of the Draft Bill, TRM Notices and Consultation Paper

***Threshold for Notification***

14.2 As mentioned in Section 3.11, it appears that similar FIs are regulated by both the TRM Notices and the Draft Bill, and thus they may face investigation from MAS and CSA respectively in the event of a data breach.

14.3 In addition, the threshold for notification under the TRM Notices is similar to that under that Draft Bill, but appears to be higher than that proposed in the Consultation Paper. The PDPC has proposed organisations notify affected individuals and PDPC of a data breach that poses any risk of impact or harm to the affected individuals.[96] Moreover, organisations must notify PDPC where the scale of the data breach is significant (i.e. more than 500 individuals), even if the breach does not pose any risk of impact or harm to the affected individuals.[97]

14.4 In this respect, the threshold set out in the Consultation Paper is significantly lower than that set out under the TRM Notices as well as the Draft Bill due to the broad and extensive category of "any risk of harm" and the additional scale of data breach criteria even in the absence of any risk of harm.

14.5 On the other hand, under Sections 10 and 15 of the Draft Bill, CIIOs must notify the Commissioner of the following:

(a) Any (significant) cybersecurity incident in respect of the CII;

(b) Any (significant) cybersecurity incident in respect of any computer/computer system under the CIIO's control that is interconnected with or communicates with the CII;

(c) Any (significant) cybersecurity incident of a type as prescribed by notification or as specified by the Commissioner.

14.6 Such breach notification criteria is similar to those defined under the TRM Notices, which requires organisations to notify MAS in the event of a relevant incident, with a relevant incident being defined in Section 2 as:

*a system malfunction or IT security incident, which has a severe and widespread impact on the bank's operations or materially impacts the bank's service to its customers.*

14.7 However, one area of notification unique to the Draft Bill is notification in the event of a change in CIIO. According to Section 14 of the Draft Bill,

*14.—(1) An owner of a critical information infrastructure must inform the Commissioner of any intended change in ownership of the critical information infrastructure, not later than 90 days before the date of the intended change in ownership.*

14.8 Thus, this additional area of notification unique to the Draft Bill will have to be taken into account in the process of harmonising the TRM Notices with the Draft Bill and the Consultation Paper.

[96] Section 6.2(a), Public Consultation for Approaches to Managing Personal Data In the Digital Economy.
[97] Section 6.2(b), Public Consultation for Approaches to Managing Personal Data In the Digital Economy.

During the roundtable, it was suggested that FIs still be required to conform to this area of notification even if they are granted particular exemptions from the Draft Bill.

***Timeline for Notification***

14.9 In fact, the timelines for notification under the TRM Notices are sufficiently onerous, given that they are required to notify MAS as soon as possible, but not later than one hour, upon the discovery of a relevant incident. In addition, FIs shall, within 14 days or such longer period as MAS may allow, from the discovery of the relevant incident submit a root cause and impact analysis report to MAS.

14.10 These notification timelines are more stringent than what the Draft Bill recommends, given that it has not stipulated any timelines for notification yet.

14.11 Moreover, the notification timelines under the TRM Notices appear to be even more exacting than those recommended by the PDPC in the Consultation Paper. Where a data breach meets the criteria for notifying PPDC and/or affected individuals under the PDPA, the PDPC proposes a timeline of only 'as soon as practicable'[98] and no later than 72 hours from the time the organisation is aware of the data breach[99] respectively.

***Legal Status***

14.12 The TRM Notices, Draft Bill and Consultation Paper are all eventually legally binding.

14.13 Under Sections 46, s46ZK, s81R, s101 and s293 of the SFA which TRM Notice CMG-N02 is pursuant to, any FI, without reasonable excuse, contravenes a direction issued by the MAS, shall be guilty of an offence. On conviction, the FI will be liable to fines depending on the type of FI concerned, with the most onerous fines not exceeding $150,000. In the case of a continuing offence, the FI will be subject to a further fine not exceeding $15,000 for every day or part thereof during which the offence continues after conviction.

14.14 Under the Banking Act which TRM Notice 644 is pursuant to, Section 55 read together with Section 71 provides a general penalty of a fine not exceeding $100,000 In the case of a continuing offence, banks contravening any provisions of the Act are subject to a further fine not exceeding $10,000 for every day or part thereof during which the offence continues after conviction.

14.15 Under the Draft Bill, any CIIO who fails to comply with any of the notification requirements shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 2 years or to both.[100]

(a) Where an offence under the Draft Bill committed by a body corporate is proved:
    (i) to have been committed with the consent or connivance of an officer; or
    (ii) to be attributable to any neglect on the officer's part, the officer as well as the body corporate shall be guilty of the offence and shall be liable to be proceeded against and punished accordingly.[101]

(b) Where, in a proceeding for an offence under the Draft Bill, it is necessary to prove the state of mind of a corporation in relation to a particular conduct, evidence that:

[98] Section 6.12, Public Consultation for Approaches to Managing Personal Data In the Digital Economy.
[99] Section 6.13, Public Consultation for Approaches to Managing Personal Data In the Digital Economy.
[100] Section 14(2), Draft Cybersecurity Bill, Singapore.
[101] Section 39(1), Draft Cybersecurity Bill, Singapore.

(i) an officer, employee or agent of the corporation engaged in that conduct within the scope of his or her actual or apparent authority; and
(ii) the officer, employee or agent had that state of mind, is evidence that the corporation had that state of mind.[102]

14.16 With regards to the Consultation Paper, while the PDPC does not propose the amount of penalty for breaching the notification requirement, there is a general penalty within the PDPA where no penalty is expressly provided of a fine not exceeding $10,000 or imprisonment for a term not exceeding 3 years or to both. In the case of a continuing offence, the organisation or individual will be subject to a further fine not exceeding $1,000 for every day or part thereof during which the offence continues after conviction.[103]

***System Readiness Requirements***

14.17 In addition, both the Draft Bill as well as the TRM Notices do regulate the operational readiness and systems compliance of organisations under their purview, namely the CIIOs and the FIs. The following table sets out the system readiness requirements of both regulations.

| TRM Notices | System Readiness Requirements | Draft Bill |
|---|---|---|
| ≤ 4 hours within 12 months[104] | **Maximum unscheduled critical system[105] / CII downtime** | None |
| ≤ 4 hours[106] | **Recovery time objective ("RTO") (per critical system / CII)** | None |
| System recovery testing/RTO validation: At least once every 12 months[107] | **System/Compliance checks** | CII compliance audit: At least once every 3 years[108] |
| | | CII cybersecurity risk assessment: At least once every 3 years[109] |
| | | Compliance audit report: ≤ 30 days[110] |

Table 3: System readiness requirements set out by the TRM Notices and the Draft Bill

14.18 It appears that the system readiness requirements set out by the TRM Notices governing FIs are far more stringent than those stipulated by the Draft Bill. For example, while the TRM Notices require FIs to ensure that the maximum unscheduled downtime for each critical system that affects the FI's operations or service to its customers does not exceed a total of 4 hours within any period of 12 months, the Draft Bill has no similar provisions in place to regulate CII failure.

[102] Section 40(1), Draft Cybersecurity Bill, Singapore.
[103] Section 56, PDPA, Singapore.
[104] Section 5, TRM Notices 644/CMG-N02.
[105] "Critical system" in relation to a bank/financial institution, means a system, the failure of which will cause significant disruption to the operations of the bank or materially impact the bank's service to its customers, such as a system which processes transactions that are time critical or provides essential services to customers.
[106] Section 6, TRM Notices 644/CMG-N02.
[107] Ibid.
[108] Section 16(1)(a), Draft Cybersecurity Bill, Singapore.
[109] Section 16(1)(b), Draft Cybersecurity Bill, Singapore.
[110] Section 16(2) Draft Cybersecurity Bill, Singapore.

14.19 In addition, the TRM Notices stipulate that FIs must establish a recovery time objective (RTO) of not more than 4 hours for each critical system, but the Draft Bill has no similar provisions in place either.

14.20 On the other hand, the Draft Bill does require CIIs to conduct a compliance audit of the CII with respect to the Draft Bill, codes of practice and standards of performance, conduct a cybersecurity risk assessment of the CII, and furnish a copy of the respective reports to the Commissioner within 30 days.

14.21 However, the TRM Notices do require FIs to validate and document at least once every 12 months how they perform their system recovery testing and when the RTO is validated during the system recovery testing.

14.22 Overall, the TRM Notices do appear to regulate FIs far more stringently than the Draft Bill, and thus having FIs comply only with the MAS regulatory regime governed by the TRM Notices may suffice.

## 10. Precedents for exempting Financial Institutions from the Draft Cybersecurity Bill

15.1 In the August 2017 Consultation by the UK Government to implement the Security of Network and Information Systems Directive ("NIS Directive")[111] adopted by the European Parliament on 6 July 2016, FIs have been exempted as the regulatory requirements they are subject to are at least equivalent to those specified in the NIS Directive.[112]

15.2 The NIS Directive[113] is the first piece of EU-wide legislation on cybersecurity, and it was implemented to ensure that providers of essential services and digital services have appropriate cyber protections. According to the NIS Directive, competent authorities or the computer security incident response teams ('CSIRTs') should receive notifications of incidents.[114]

15.3 However, as Principle 11 under the Principles of Business of the legally binding Financial Conduct Authority (FCA) Handbook[115] already requires financial services organisations regulated by the FCA to disclose 'anything relating to that firm of which the regulator would reasonably expect notice', FIs were exempted from being subject to similar regulatory requirements under the NIS Directive.

## 11. Collaborative notifications from financial institutions to regulators

16.1 In accordance with the current regulatory regimes, should FIs experience a cybersecurity incident, including data breaches, they will have to notify the MAS, CSA and PDPC under the TRM Notices, Draft Bill, and the PDPA (if the Consultation Paper proposals are accepted) respectively. Consequently, they may also be subject to investigations from these three regulators and other law enforcement agencies, which appears to be onerous and may result in increased time costs for FIs involved.

---

[111] Consultation by the UK Government to implement the Security of Network and Information Systems Directive, issued 8 August 2017.
[112] Section 3, Consultation by the UK Government to implement the Security of Network and Information Systems Directive, United Kingdom.
[113] Directive on Security of Network and Information Systems, adopted by the European Parliament on 6 July 2016.
[114] Article 14(3), Directive on Security of Network and Information Systems, European Union.
[115] SUP 15.3.7, FCA Handbook, United Kingdom.

16.2 Currently, the PDPC has proposed in its Consultation Paper for the mandatory data breach notification requirements under the PDPA to apply concurrently with other notification requirements under other laws and sectoral regulations in the following manner:

(a) Where the organisation is required to notify a sectoral or law enforcement agency of a data breach under other written law, and that data breach meets the criteria for notifying the PDPC, it is proposed that the organisation shall notify PDPC concurrently with the sectoral regulator or law enforcement agency in accordance with the notification requirements under the other written law. In such cases, the organisation may submit to the PDPC the same notification or copy the PDPC in its notification to the sectoral or law enforcement agency. This is to minimise the effort and cost involved to comply with notification requirements for the same data breach, while allowing PDPC to continue to be kept informed of data breaches of potential concern.[116]

16.3 Nonetheless, FIs will still be subject to investigation from the PDPC in the event of a data breach.

16.4 The diagram below sets out the current regulatory regime, taking into account the Draft Bill and the Consultation Paper.

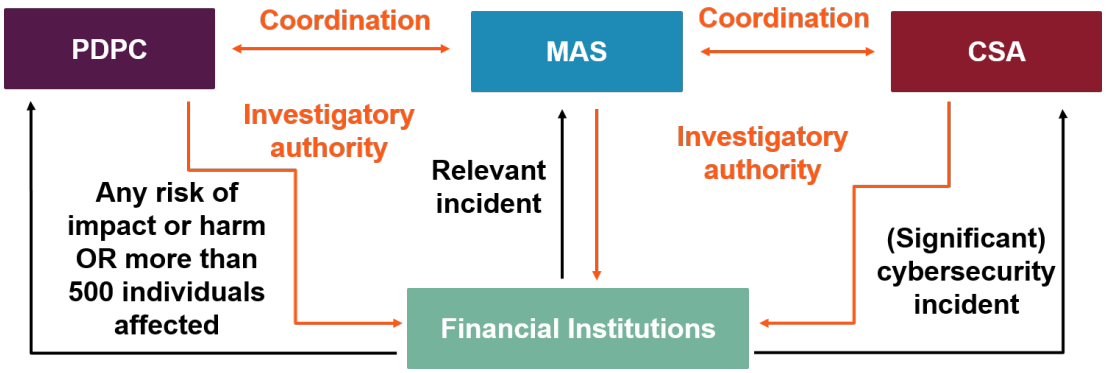


Fig 1: Current investigation and reporting structure for FIs (taking into account the Draft Bill and Consultation Paper)

16.5 Based on our findings, we thus propose for the exemption of FIs from the regulatory requirements of the Draft Bill. As mentioned in Sections 14.5 and 14.6, the definitions of "relevant incident" and "(significant) cybersecurity incident" are similar. Both the TRM Notices and the Draft Bill thus appear to regulate similar incidents, and it might ease the regulatory burden on FIs if they are required to report to only two regulators – the PDPC and MAS.

16.6 Moreover, the threshold and timeline for notification as well as the system readiness requirements under the TRM Notices are sufficiently onerous and more stringent than the Draft Bill. In addition, both the TRM Notices and the Draft Bill are legally binding and have similar penalties for non-compliance, thus exempting FIs from the Draft Bill will not absolve them of legal ramifications should they be found guilty of non-compliance with the TRM Notices.

16.7 Lastly, the Consultation Paper provides for greater personal data protection, and when taken together with the TRM Notices, will provide sufficient safeguards for consumers with regard to FIs.

[116] Section 6.3(a), Public Consultation for Approaches to Managing Personal Data In the Digital Economy.

16.8 Hence, the following table sets out our proposed reporting and investigatory structure for FIs with regard to the TRM Notices, Consultation Paper and Draft Bill.

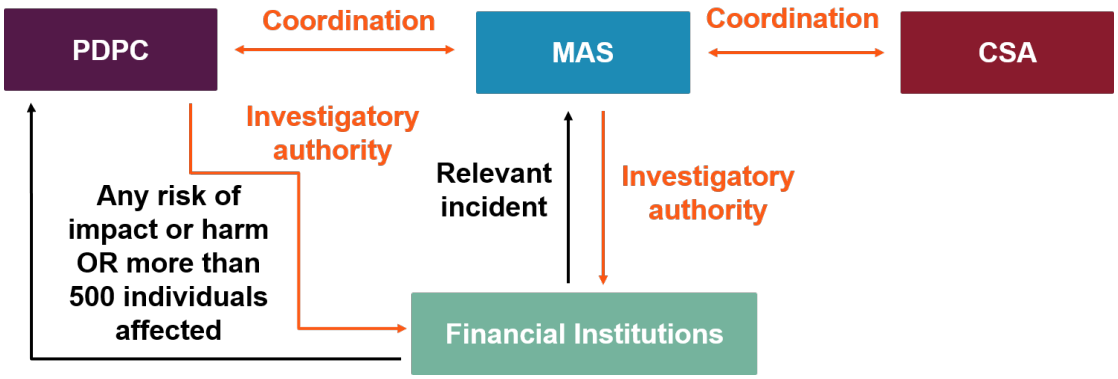


Figure 2: Proposed investigation and reporting structure for FIs (taking into account the Draft Bill and Consultation Paper)

16.9 In our proposed investigation and reporting structure, FIs will be exempted from complying with the Draft Bill, with the exception of notifying the Commissioner of any intended change in ownership of the CII not later than 90 days before the date of the intended change in ownership. This is because this clause is not covered in either the PDPA, Consultation Paper or the TRM Notices.

16.10 However, they will still be required to notify PDPC and MAS under the PDPA (and the Consultation Paper proposals) and the TRM Notices respectively, and be subject to investigations from both regulatory authorities in the event of a data breach or other cybersecurity incidents. At the regulatory level, the PDPC, MAS and CSA can work closely and collaborate with each other to enhanced the data protection and cybersecurity regulatory regime in Singapore.

16.11 This will thus help to ease the regulatory burden on FIs and promote Singapore as an efficient and conducive financial hub.

## 12. Collaborative investigations from regulators

17.1 As mentioned in Section 16.11, FIs will still be subject to investigations from the PDPC and MAS in the event of a relevant incident involving personal data, and investigations from the PDPC in the event of a data breach that is not a relevant incident as defined in the TRM Notices. However, given the broad definition of a relevant incident which includes a "material impact" on the FI's service to customers, it is highly likely that in any incident both regulatory agencies will be involved.

17.2 Nonetheless, this still reduces the regulatory burden on FIs as they will not be subject to additional regulation and investigation from the CSA.

## PART V: GENERAL

### 13. Implications on innovation

18.1 It may also be pertinent to consider the implications of such regulatory regimes on financial technology ("**FinTech**") start-up companies. As such start-ups focus on FinTech, it is likely that they will fall under the purview of the Draft Bill, TRM Notices and the Consultation Paper.

18.2 Indeed, a point raised during the roundtable was that start-ups, who may already be facing issues with obtaining enough capital and maintaining liquidity, may not have the means to obtain legal or consulting advice to comply with such rigorous regimes. Thus, this may stifle FinTech innovation in Singapore in the long run should start-ups be faced with penalties from regulatory agencies in the event of non-compliance and be forced to terminate operations.

18.3 On the other hand, Australia appears to have found a solution to this issue as it does not generally require private sector organisations to comply with Australian Privacy Principles which govern the management of personal information if they have an annual turnover of less than AUD$3,000,000.

### 14. Other general issues

***Scope of CII***

19.1 Participants during the roundtable also raised the issue of the definition of CII, given that CII may be interconnected across a diversified company carrying a broad range of businesses including the one or more essential services. Participants also raised questions of whether connecting a computer system to a CII would automatically render the former as part of the CII as well.

19.2 In addition, participants felt that there ought to be more clarification on whether third party service providers and operators should be subject to CII requirements, and whether CII regulations would extend to computer systems abroad.

***Obligations of data intermediaries regarding data breach notifications***

19.3 Participants agreed with the Consultation Paper's proposals to have data intermediaries be required to immediately inform the organisation that it processes the personal data on behalf and for the purposes of in the event of a data breach, and for the organisation to be responsible for complying with the breach notification requirements in the Consultation Paper.

***Notifying PDPC under significant scale of data breach criteria***

19.4 During the roundtable, many participants took issues with the Consultation Paper's proposal that oganisations must notify PDPC where the scale of the data breach is significant (i.e. 500 or more individuals), even if the breach does not pose any risk of impact or harm to the affected individuals.

19.5 Many felt that the significant scale of data breach criteria should not be used as a litmus test to indicate any systemic issues within the organisation. Instead, they felt the PDPC should focus on the asset class of the data which breached, rather than definite number of individuals who were affected.

19.6 In addition, some participants expressed interest in using a de minimis criteria to qualify the scale of data breach instead. In this case, organisations would only be require to notify the PDPC under the scale of breach criteria if the number of individuals was more than de minimis.

## 15. Further information

20.1 Should you require any further information, please do not hesitate to contact Koh Chia Ling at +65 6350 4382 or ChiaLing.Koh@osborneclarke.com.[117]

[117] Special thanks to Gerald Tan of London School of Economics for putting the first draft of this report together.