7-2018

Data protection in the Internet: National rapporteur (Singapore)

Ee-Ing ONG
Singapore Management University, eeingong@smu.edu.sg

QUESTIONNAIRE

Part I – General Data Protection

I. GENERAL DATA PROTECTION FRAMEWORK

1. Is there any legislation and/or relevant case law regarding personal data protection applicable in your legal system? In case the answer is affirmative, please identify the applicable legislation and/or relevant case law, if any.

2. In the event the previous answer is affirmative, please provide additional information:

2.1. What does personal data mean in the legislation (please explain if personal data protection is recognized as a specific right or if it derives from other rights such as, e.g., private life, privacy or protection of intimacy)?

2.2. Is personal data classified in categories in the legislation? In case of an affirmative answer, please indicate the categories.

2.3. Is legislation regarding personal data protection applicable to the processing of personal data by any entity or is there any category of entities with specific regulation (e.g., public entities)? In case there is a specific regulation, please discriminate its scope.

1. Response 1-2

In Singapore, personal data protection is governed by the **Personal Data Protection Act 2012** ("**PDPA**").[1] Based on international standards, this is the first comprehensive personal data protection legislation in Singapore.[2] Prior to the PDPA, sector-specific statutes covered aspects of personal data protection in a piecemeal fashion.[3] For instance, the Banking Act states that customer information shall not be disclosed by any bank in Singapore, save as provided under such act.[4] However, the sector-specific statutes "are of limited scope and application with regard to data protection" as their provisions "typically penalise the unauthorised release of personal information and are not as far reaching as the provisions of the [PDPA]," nor do they "confer private rights of action or direct remedies that are typically available under data protection laws."[5]

The PDPA governs the collection, use and disclosure of personal data by organisations, in a

[1] (No. 26 of 2012). Available via Singapore Statutes Online. https://sso.agc.gov.sg. ("PDPA.") The data protection provisions came into effect on 2 July 2014: Personal Data Protection Act 2012 (Commencement) Notification 2014 (S 361 of 2014). Available via Singapore Statutes Online. https://sso.agc.gov.sg.

[2] Singapore Parliamentary Debates, Official Report (15 October 2012) vol 89. Available via Parliament of Singapore. https://www.parliament.gov.sg. See also Chesterman S (2014) From Privacy to Data Protection (para 1.30). In: Chesterman S (ed) Data protection law in Singapore: privacy and sovereignty in an interconnected world. Academy Publishing, Singapore ("Chesterman").

[3] Chesterman para 1.30.

[4] (Cap 19, 2008 Rev Ed) at s 47(1). Available via Singapore Statutes Online. https://sso.agc.gov.sg.

[5] Ter KL (2013) Singapore's Personal Data Protection Legislation: Business Perspectives. Computer Law & Security Review 29:264-273, p 265.

manner that balances the "right of individuals to protect their personal data" with the "need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances."[6] It presents a "light touch" regime which establishes a "minimum data protection standard", and in the event of a conflict other laws shall prevail over the PDPA.[7]

An "organisation" is any individual, company, association or body of persons, whether or not formed under Singapore law, or resident or having a place of business in Singapore.[8] The PDPA generally excludes: individuals acting in a personal or domestic capacity; public agencies (including the Singapore Government and governmental organizations); [9] and employees acting in the course of their employment.[10] Some exceptions also apply for data intermediaries (see Response 13).

"Personal data" means "data (whether true or not) about an individual who can be identified (a) from that data; or (b) that data and other information to which the organisation has or is likely to have access."[11] The PDPA applies to all forms of personal data, save for: personal data about an individual in a record that has existed for at least 100 years;[12] data about a deceased individual;[13] business contact information;[14] and anonymised data.[15] (There is no specific right of privacy in Singapore, although the usual common law protections for privacy apply, eg the law of confidence and defamation.[16])

There are ten general categories of data protection, each an "Obligation" on an organisation:

- *Consent*: No collection, use, or disclosure of personal data about an individual without

[6] PDPA s 3.
[7] Chik W (2013) The Singapore Personal Data Protection Act and an Assessment of Future Trends in Data Privacy Reform. Computer Law & Security Review 29:554-575, p 558 (discussing PDPA s 4(6)).
[8] PDPA s 2(1).
[9] The Singapore Government and governmental organisations (and employees thereof) are prohibited from disclosing confidential information obtained in the course of their work by, among others, the Statutory Bodies and Government Companies (Protection of Secrecy) Act (Cap 319, 2004 Rev Ed) and the Official Secrets Act (Cap 213, 2012 Rev Ed). See also discussion on the Public Sector (Governance) Act 2018.
[10] PDPA s 4(1).
[11] PDPA s 2(1).
[12] PDPA s 4(4)(*a*).
[13] PDPA s 4(4)(*b*). The individual must have been deceased for more than 10 years.
[14] PDPA s 4(5).
[15] PDPC (2017) Advisory Guidelines on Key Concepts in the Personal Data Protection Act (para 5.3). https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/advisory-guidelines-on-key-concepts-in-the-pdpa-(270717).pdf. Accessed 12 Jan 2018. ("Advisory Guidelines on Key Concepts."). See also PDPC (2017) Advisory Guidelines on the Personal Data Protection Act for Selected Topics (chapter 3). https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/finaladvisoryguidelinesonpdpaforselectedtopics28march2017.pdf. Accessed 12 Jan 2018. ("Advisory Guidelines for Selected Topics.")
[16] See Chan G, Lee PW (2016) The Law of Torts in Singapore. Academy Publishing, Singapore ("Chan"). See also Response 12.

that individual's consent as obtained through specified procedures.[17]

- *Limited Purpose*: Collection, use or disclosure of personal data only for purposes that a reasonable person would consider appropriate and if the individual has been notified of such purposes.[18]
- *Notification*: To inform an individual of the purpose of the collection, use or disclosure of personal data.[19]
- *Access*: To give an individual access to personal data held by or under the control of the organisation, including information about how such personal data was or may have been used or disclosed within a year before the date of the request.[20]
- *Correction*: To correct an error or omission regarding personal data about that individual.[21]
- *Accuracy*: To ensure that personal data collected by or on behalf of the organisation is accurate and complete.[22]
- *Protection:* To protect personal data in the organisation's possession or under its control through reasonable security arrangements.[23]
- *Limited Retention*: To stop retaining personal data as soon as it is reasonable to assume that the purpose for which the data was collected is no longer served by such retention, and retention is no longer necessary for legal or business purposes.[24]
- *Limited Transfer*: No transfer of personal data outside Singapore, save if the transferred personal data will enjoy protection comparable to the protection under the PDPA.[25]
- *Openness*: To implement data protection policies and practices, and appoint a data protection officer.[26]

There are no specified standards for the Obligations. Instead, organisations may collect, use and disclose data "for purposes which a reasonable person would consider appropriate in the circumstances."[27] A "'reasonable person' is judged based on an objective standard and can be said to be a person who exercises the appropriate care and judgement in the particular circumstances."[28]

The PDPA does not apply to government agencies. Instead, data sharing by Singapore government agencies is governed specifically under the **Public Sector (Governance) Act 2018 (PS(G)A)**.[29] The PS(G)A is intended to be in alignment with the PDPA, including to "significantly improve the protection and safeguard of such shared data."[30] Under this act,

[17] PDPA s 13-16. See Response 6-7.
[18] PDPA s 18.
[19] PDPA s 20(1).
[20] PDPA s 21(1).
[21] PDPA s 22.
[22] PDPA s 23.
[23] PDPA s 24.
[24] PDPA s 25.
[25] PDPA s 26.
[26] PDPA s 11-12.
[27] Advisory Guidelines on Key Concepts para 9.3. See, eg, PDPA ss 11(1), 18, 24, 25.
[28] Advisory Guidelines on Key Concepts para 9.5.
[29] No 8 of 2018. Available via Singapore Statutes Online. https://sso.agc.gov.sg.
[30] Singapore Parliamentary Debates, Official Report (8 January 2018) vol 94. Available via Parliament of Singapore. https://www.parliament.gov.sg.

where a "data sharing direction"[31] is given, a Singapore public sector agency is generally authorised to share information under its control with another Singapore public sector agency.[32] However, such direction must not be inconsistent with any other written law.[33] The Public Sector (Governance) Act will likely be administered by the Prime Minister's Office.[34]

Other key statutes which affect personal data are discussed in the rest of the Questionnaire:

- Computer Misuse and Cybersecurity Act (Responses 6-7; 20-21; 22-23; 24-25; 26; 27);
- Criminal Procedure Code (Responses 6-7; 20-21; 22-23; 24-25; 26; 27);
- Cybersecurity Act (Responses 6-7; 20-21; 22-23; 24-25; 26; 27);
- Telecommunications Act (Responses 16-17; 18-19; 22-23);
- Electronic Transactions Act (Responses 16-17; 18-19);
- Spam Control Act (Response 8-9).

3. Is there any entity supervising or controlling, in any way, the processing of personal data (including, e.g., an entity which has taken upon itself this role and which, at least to some extent, plays this role de facto, though not de jure)?

4. In the event the previous answer is affirmative, please provide additional information (referring the applicable legislation and relevant case law, if any):

4.1. Is supervision conducted by one single general supervisory body or are there sectorial supervisory bodies (please identify these bodies, if any)?

4.2. Please indicate the main powers vested in the supervisory body or bodies, including sanctioning powers.

2. Response 3-4

The PDPA is directly administered by the **Personal Data Protection Commission ("Commission"** or **"PDPC").**[35] The Commission is overseen by the Info-communications Media Development Authority ("IMDA"), and the IMDA in turn comes under the Ministry of Communications and Information ("MCI").[36]

The Commission may conduct investigations regarding alleged non-compliance of the PDPA,[37] and including requiring documents and information, inspecting premises,[38] and

[31] "Data sharing direction" means a direction issued under the PS(G)A regarding "sharing of information or re-identification of anonymised information under the control of a Singapore public sector agency." PS(G)A s 2(1).
[32] PS(G)A s 6(1).
[33] PS(G)A s 11(1).
[34] See Public Consultation on the Public Sector (Governance) Bill <https://www.reach.gov.sg/participate/public-consultation/prime-ministers-office/public-service-division/public-consultation-on-the-public-sector-governance-bill>; Media Factsheet On The Public Sector (Governance) Bill <http://www.nas.gov.sg/archivesonline/data/pdfdoc/20180108011/Media%20factsheet%20on%20the%20Public%20Sector%20-%20Governance-%20Bill.pdf>. Accessed 12 Jan 2018.
[35] PDPA s 5, 6(g).
[36] MCI (2017) Agencies. https://www.mci.gov.sg/agencies. Accessed 12 May 2017.
[37] PDPA s 50.
[38] PDPA Ninth Schedule.

imposing certain remedies and sanctions[39] (see Response 24-25).The Commission shall also: promote awareness of data protection in Singapore; provide advisory services (including to the Singapore Government) regarding data protection; conduct research and educational activities regarding data protection; and manage technical co-operation regarding data protection with foreign, international, and governmental authorities.[40]

The Commission has issued a large number of advisory guidelines on the PDPA:[41] general guidelines, sector-specific guidelines, and guidelines on specific topics (including managing data breaches and securing personal data in electronic medium). While technically non-binding[42] these guidelines are carefully studied by other government agencies,[43] lawyers,[44] and industry players.[45] Additionally, the Commission has begun making reference to its own advisory guidelines in the cases it adjudicates.[46]

These guidelines are also updated from time to time. For instance, the Commission recently held a public consultation on "Approaches to Managing Personal Data in the Digital Economy", and the results will be implemented in 2018-19.[47]

---

[39] PDPA s 29.
[40] PDPA s 6.
[41] PDPC (2018) Guidelines. https://www.pdpc.gov.sg/Legislation-and-Guidelines/Guidelines. Accessed 12 Jan 2018.
[42] PDPA s 49(3).
[43] See eg, Cyber Security Agency of Singapore "PDPC Guides" https://www.csa.gov.sg/gosafeonline/resources/pdpc-guides (Accessed 19 June 2018).
[44] See eg, Hogan Lovells' report "New PDPC guidance on data management practices in Singapore", https://www.hoganlovells.com/en/publications/new-pdpc-guidance-on-data-management-practices-in-singapore (Accessed 19 June 2018); CNP Law's report on "Personal Data Protection Committee issues sector specific advisory guidelines", https://www.cnplaw.com/personal-data-protection-committee-issues-sector-specific-advisory-guidelines/ (Accessed 19 June 2018).
[45] See eg, the Singapore Council for Estate Agencies' website which contains links to the relevant advisory guidelines, and which encourages property agencies and agents to familiarize themselves with these and other PDPC advisory guidelines, https://www.cea.gov.sg/legislation-guidelines/practice-guidelines-circulars/personal-data-protection. (Accessed 7 June 2018); "Singapore: PDPC data management guides "emphasise accountability" https://www.dataguidance.com/singapore-pdpc-issues-guides-emphasising-accountability-data-management/ (Accessed 19 June 2018); "Personal Data Protection Commission issues advisory guidelines on in-vehicle recording" https://www.opengovasia.com/articles/personal-data-protection-commission-issues-advisory-guidelines-on-in-vehicle-recording (Accessed 19 June 2018).
[46] See, eg, *Furnituremart.sg* [2017] SGPDPC 07; *Spring College International Pte. Ltd.* [2018] SGPDPC 15.
[47] PDPC (2018) Public Consultation for Approaches to Managing Personal Data in the Digital Economy https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/publicconsultationapproachestomanagingpersonaldatainthedigitaleconomy270717f95e65c8844062038829ff000.pdf. Accessed 18 June 2018; PDPC (2018) Response to Feedback on the Public Consultation on Approaches to Managing Personal Data in the Digital Economy. https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Legislation-and-Guidelines/PDPC-Response-to-Feedback-for-Public-Consultation-on-Approaches-to-

5. What is the relevance, if any, of self-regulation instruments on data protection in your jurisdiction?

Response 5

Various industries have incorporated aspects of the PDPA (including the advisory guidelines) into their codes of conduct and industry guides. See Response 15.

Part II – Data Protection in the Internet

II. PERSONAL DATA PROCESSED BY ELECTRONIC MEANS

6. Is there any legislation and/or relevant case law covering the protection of personal data in the context of services provided at a distance, by electronic means, at the individual request of a recipient of services (including rules concerning the protection of personal data in social networks)? In case the answer is affirmative, please identify the applicable legislation and/or relevant case law (please discriminate if it is a general legislation or case law, which also covers that context, or if it is a specific legislation or case law).

7. In the event the previous answer is affirmative, please provide additional information:

7.1 Any additional/specific protection for the data subject in that context (e.g., mandatory information provided in a durable medium).

7.2. Is the previous consent of the data holder required for the electronic processing of personal data? In the event a previous consent is necessary, as a rule, please specify which circumstances, if any, may determine the electronic processing without this consent (e.g., the processing to protect legitimate interests of the data controller, such as the processing of dynamic IP addresses to prevent cyberattacks and make it possible to bring criminal proceedings against those responsible).

7.3. Is the electronic processing of personal data limited to specific purposes or to specific types of data or are there particular requirements for the electronic processing of specific purposes or specific types of data?

7.4. Any specific protection for minors (e.g., the control of the age of the recipient of the service; different requirements depending on the age; the necessary participation of legal representatives).

7.5. Any specific rules for the rectification and/or erasement of data previously processed with the consent of the data subject («right to be forgotten»).

Response 6-7

(i) Consent

The PDPA covers all personal data, whether in electronic or other form.[48]

Organisations may not collect, use or disclose an individual's personal data unless the

Managing-Personal-Data-in-the-Dig.pdf. Accessed 18 June 2018. ("Public Consultation June 2018.")

[48] Advisory Guidelines on Key Concepts para 5.2, 5.30.

individual has given, or is deemed to have given, his consent, save for exceptions discussed below.[49]

An individual has not given consent unless he/she has been notified of the purposes of the collection, use or disclosure of the personal data and given consent for such purposes; and been provided (on request) with the business contact information of a person who can answer the individual's questions about the collection, use or disclosure of the personal data.[50]

An organisation collecting personal data about an individual from another organisation without the individual's consent shall provide such other organisation with sufficient information regarding the purpose of such collection, to allow such other organisation to determine if the disclosure would be in accordance with the PDPA.[51]

The PDPA does not prescribe the manner of obtaining consent, although it is "good practice" to obtain written consent.[52] However, an organisation shall not require consent as a condition of providing a product or service "beyond what is reasonable to provide the product or service"; or obtain consent by providing "false or misleading information" or "using deceptive or misleading practices".[53] Consent obtained under such circumstances is invalid.[54]

Factors in determining whether it is reasonable for an organisation to require consent as such a condition of providing a product or service include: the amount and type of personal data sought; the purpose of the collection, use or disclosure of the personal data; the nature of the item being provided, including whether there is any benefit tied to the item (eg whether the item is being provided without monetary payment to the organisation); and what a reasonable person would consider appropriate in the circumstances.[55]

- For example, "organisations may provide offers, discounts or lucky draw opportunities to individuals that are conditional on the collection, use or disclosure of their personal data for specified purposes."[56]

When Consent is Not Required

Consent is not required if: (a) the individual is deemed to have given consent; or (b) an exception applies.[57]

(a) Deemed consent.

An individual is deemed to have consented to the collection, use or disclosure of his/her personal data for a purpose if the individual voluntarily provides such data to the organisation

[49] PDPA s 13.
[50] PDPA s 14(1) read with s 20(1).
[51] PDPA s 20(2).
[52] Advisory Guidelines on Key Concepts para 12.5.
[53] PDPA s 14(2).
[54] PDPA s 14(2)-(3).
[55] PDPC (2015) Advisory Guidelines on Requiring Consent for Marketing Purposes (para 5.2). https://www.pdpc.gov.sg/docs/default-source/advisory-guidelines-on-consent-for-mktg/advisory-guidelines-on-requiring-consent-for-marketing-(8-may-2015).pdf. Accessed 12 Jan 2018. ("Advisory Guidelines on Requiring Consent for Marketing Purposes.")
[56] Advisory Guidelines on Requiring Consent for Marketing Purposes para 7.2.
[57] PDPA s 13.

for that purpose and it is reasonable that the individual would voluntarily provide the data.[58]

Additionally, if the individual gives (or is deemed to give) consent for disclosure of his/her personal data by one organisation to another organisation for a particular purpose, he/she is deemed to consent to the collection, use or disclosure of such data for such purpose by that other organisation.[59]

- For instance, if an individual booking a taxicab is asked for his/her name and telephone number in order to inform him/her of the taxicab number, and the individual voluntarily provides such information, then the individual is deemed to have consented to the taxicab company using her name and number to notify her when the taxicab arrives.[60] However, the individual is not deemed to have consented to the use of his/her name and number for other purposes, eg the marketing of a limousine service run by the cab company.[61]

Recently, pursuant to a public consultation in July 2017, there will be an additional category of consent termed "Deemed Consent by Notification."[62] This will be allowed where:

- the organisation notifies individuals of the purpose of collecting, using and disclosing their data,
- the individual is provided a reasonable time period to opt-out but does not opt-out within the time period, and
- such collection, use or disclosure is not likely to have any adverse impact on the individuals.[63]

The organisation must also first conduct a risk and impact assessment, such as a data protection impact assessment, to ascertain whether such collection, use or disclosure is likely to have any adverse impact on the individual.[64]

(b) When consent is not required.

Consent is not required if the collection, use or disclosure of data is: necessary for any purpose that is "clearly in the interests of the individual" and if consent cannot be timely obtained or the individual would not reasonably be expected to withhold consent;[65] for an emergency threatening the life, health or safety of any individual;[66] for personal data which is publicly available;[67] in the national interest[68] or necessary for investigation or proceedings;[69] necessary for evaluative purposes;[70] or necessary to recover debt owed from an individual to the

[58] PDPA s 15(1).
[59] PDPA s 15(2).
[60] Advisory Guidelines on Key Concepts para 12.24.
[61] Advisory Guidelines on Key Concepts para 12.24.
[62] Public Consultation June 2018 (Part II).
[63] Public Consultation June 2018 (Part II).
[64] Public Consultation June 2018 (para 4.2).
[65] PDPA Second Schedule s 1(a), Third Schedule s 1(a), Fourth Schedule 1(a) (save that there is no requirement for disclosure that the individual not reasonably be expected to withhold consent).
[66] PDPA Second Schedule s 1(*b*), Third Schedule s 1(*b*), Fourth Schedule 1(*b*)-(*c*).
[67] PDPA Second Schedule s 1(*c*), Third Schedule s 1(*c*), Fourth Schedule 1(*d*).
[68] PDPA Second Schedule s 1(*d*), Third Schedule s 1(*d*), Fourth Schedule 1(*e*).
[69] PDPA Second Schedule s 1(*e*), Third Schedule s 1(*e*), Fourth Schedule 1(*f*).
[70] PDPA Second Schedule s 1(*f*), Third Schedule s 1(*f*), Fourth Schedule 1(*h*).

organisation or vice versa[71] or to provide or obtain legal services.[72] Other exceptions apply, eg regarding personal data for business asset transactions;[73] credit bureaus;[74] employment purposes;[75] news activities;[76] and research purposes.[77]

Pursuant to a public consultation in July 2017, there will be an additional exception for "Legitimate Interests."[78] Organisations will be able to collect, use or disclose personal data where there is a need to protect legitimate interests that will have economic, social, security or other benefits, so long as the benefits to the public clearly outweigh any adverse impact to the individuals involved.[79] Organisations wishing to use this exception will also need to conduct a risk and impact assessment to determine whether the benefits outweigh any foreseeable adverse impact to the individual.[80] While the term "Legitimate Interests" tracks the language adopted in the EU GDPR, the Commission will provide its own guidelines on the term.[81]

Withdrawing Consent

An individual may at any time, with reasonable notice, withdraw consent given or deemed given.[82] The organisation shall inform the individual of the likely consequences of such action, but without prohibiting him/her from such action; however, such withdrawal shall not affect any legal consequences from such withdrawal.[83]

- For example, a telecoms service provider provides subscriber services requiring the collection, use and disclosure of personal data.[84] The subscriber provides consent to the above but subsequently withdraws it.[85] Such withdrawal will result in the operator being unable to provide said services, ie early termination of the service contract; thus the operator should inform the individual of the consequences, ie incurrence of early termination charges.[86]
- Additionally, where an organisation provides a facility for individuals to withdraw consent, eg by clicking on an "unsubscribe" link within an e-mail, the organisation should indicate the scope of such withdrawal.[87] For instance, a statement that "[y]ou have unsubscribed successfully from e-mail marketing messages from ABC" means that the individual has only withdrawn consent to marketing messages sent by e-mail, and not by fax.[88]

Upon withdrawal, the organisation shall also cease (and cause its data intermediaries and agents

[71] PDPA Second Schedule s 1(*i*), Third Schedule s 1(*g*), Fourth Schedule 1(*i*).
[72] PDPA Second Schedule s 1(*j*), Third Schedule s 1(*h*), Fourth Schedule 1(*j*).
[73] PDPA Second Schedule s 1(*p*), Third Schedule 1(*j*), Fourth Schedule s 1(*p*).
[74] PDPA Second Schedule s 1(*k*), Third Schedule 1(*j*), Fourth Schedule 1(*k*).
[75] See Response 10-11.
[76] PDPA Second Schedule 1(*h*), Third Schedule 1(*j*), Fourth Schedule 1(*s*).
[77] PDPA Third Schedule s 1(*i*), Third Schedule 1(*j*), Fourth Schedule (*s*).
[78] Public Consultation June 2018 (Part II).
[79] Public Consultation June 2018 (Part II).
[80] Public Consultation June 2018 (Part II).
[81] Public Consultation June 2018 (para 5.6).
[82] PDPA s 16(1).
[83] PDPA s 16(2)-(3).
[84] Advisory Guidelines on Key Concepts para 12.45.
[85] Advisory Guidelines on Key Concepts para 12.45.
[86] Advisory Guidelines on Key Concepts para 12.45.
[87] Advisory Guidelines on Key Concepts para 12.48.
[88] Advisory Guidelines on Key Concepts para 12.48.

to cease) collecting, using or disclosing such personal data, subject to exceptions under the PDPA or other law.[89] Withdrawal of consent does not require deletion or destruction of the individual's personal data, save as required under the Limited Retention Obligation (see Response 13).[90]

There is no specific right to be forgotten. However, see Response 13 on the Limited Retention Obligation.

(ii) Access

An organisation shall provide, on an individual's request: personal data about the individual in the organisation's possession or control; and information about the ways in which such data has or may have been used or disclosed by the organisation within a year before the date of the request.[91] An organisation can charge reasonable fees for access.[92]

Exceptions. Access shall not be provided if provision of that data or information could reasonably be expected to: threaten the safety or physical or mental health of another individual; cause immediate or grave harm to the safety or physical or mental health of another individual; reveal personal data about another individual; reveal the identity of an individual who has provided personal data about another individual and the former does not consent to disclosure of his/her identity; or be contrary to the national interest.[93] An organisation shall also not inform an individual that it has disclosed personal data to a law enforcement agency, if such disclosure was made without that individual's consent (as allowed under the Fourth Schedule or other law).[94]

Access is also not required regarding, eg: opinion data kept solely for an evaluative purpose; school examinations; personal data subject to legal privilege; personal data collected, used or disclosed without consent for the purposes of an investigation in progress; "confidential commercial information" that could, in the opinion of a reasonable person, harm the organisation's competitive position; and repetitious requests "that would unreasonably interfere with the operations of an organisation."[95]

However, access shall be given to an individual's personal data and information if such data or information can be stripped of the abovementioned prohibited data and information.[96]

(iii) Correction

An individual may request an organisation to correct an error or omission in his/her personal data in the possession or control of the organisation.[97] Unless the organisation is "satisfied on reasonable grounds" that a correction should not be made (in which case it shall annotate the

[89] PDPA s 16(4).
[90] PDPA s 16(4); Advisory Guidelines on Key Concepts para 12.55.
[91] PDPA s 21(1).
[92] Personal Data Protection Regulations 2014 (S 362 of 2014) s 7(1). Available via Singapore Statutes Online. https://sso.agc.gov.sg. ("PDPR.") See also Advisory Guidelines on Key Concepts para 15.19.
[93] PDPA s 21(3).
[94] PDPA s 21(4).
[95] PDPA Fifth Schedule s 1.
[96] PDPA s 21(5).
[97] PDPA s 22(1).

personal data with the correction that was requested but not made),[98] it shall correct the data and send it to "every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction was made".[99] Fees may not be charged for such correction.[100]

Exceptions. An organisation need not correct an opinion, including a professional or expert opinion.[101] Correction is also not required regarding, eg: opinion data kept solely for evaluative purposes; school examinations; and documents related to a prosecution if proceedings have not been completed.[102]

(iv) Limited Purpose

An organisation may collect, use or disclose personal data about an individual only for purposes that "a reasonable person would consider appropriate in the circumstances" and of which the individual has been notified.[103] A purpose that is in violation of law or which would be harmful to the individual concerned is unlikely to be considered appropriate by a reasonable person.[104]

(v) Minors

The PDPA does not specify when a minor (an individual less than 21 years-old) may give consent.[105] Instead, whether a minor can give consent would depend on other relevant laws.[106] In general, the rights of parents in respect of their children are derived from the common law but there may be legislation that affects how and if they may exercise such rights.[107] However, the Commission has specifically issued guidelines on obtaining a minor's consent.[108]

For instance, organisations should consider whether a minor has "sufficient understanding of the nature and consequences of giving consent."[109] The rule of thumb (based in part on the United States Children's Online Privacy Protection Act[110] and the Singapore Employment Act[111]) is that an individual who is at least 13 years-old would have sufficient understanding to consent on his/her own behalf.[112] However, where there is reason to believe or it can be shown that a minor 13 or over does not have sufficient understanding of the nature and consequences of giving consent, or the minor is under 13, the organisation should obtain consent from an individual legally able to provide consent on the minor's behalf, such as a parent or guardian.[113]

---

[98] PDPA s 22(2) read with (5).
[99] PDPA s 22(2).
[100] Advisory Guidelines on Key Concepts para 15.39.
[101] PDPA s 22(6).
[102] PDPA Sixth Schedule s 1.
[103] PDPA ss 18 read with 20.
[104] Advisory Guidelines on Key Concepts para 13.4.
[105] Advisory Guidelines for Selected Topics para 8.1.
[106] Advisory Guidelines for Selected Topics para 8.1 (discussing PDPA s 4(6)(*a*)).
[107] Advisory Guidelines for Selected Topics para 8.7.
[108] Advisory Guidelines for Selected Topics paras 8.1-8.13.
[109] Advisory Guidelines for Selected Topics para 8.6.
[110] 15 USC Chapter 91. Available at https://www.law.cornell.edu/uscode/text/15/chapter-91.
[111] (Cap 91, 2009 Rev Ed). Available via Singapore Statutes Online. https://sso.agc.gov.sg.
[112] Advisory Guidelines for Selected Topics paras 8.3-8.6.
[113] Advisory Guidelines for Selected Topics paras 8.6, 8.9.

Deemed consent. While the 13-year-old threshold would still apply, organisations wishing to rely on deemed consent should take extra care to establish whether such minor has sufficient understanding of the purposes for which the organisation is collecting, using and disclosing data and the consequences of giving his/her data.[114] Organisations should also not exercise undue influence to obtain personal data from minors.[115]

(vi) Personal data on computers

In addition to the PDPA and abovementioned advisory guidelines, Singapore also has laws involving the investigation of personal data on computers (including web-based servers). The authorities' computer-related powers of investigation under the **Criminal Procedure Code**[116] were significantly enhanced under recent amendments, as investigators can during an investigation:

- Inspect and search any data stored on or available to a computer implicated in the investigation, regardless of whether the computer is inside or outside Singapore (thus this could include web-based email accounts and web storage accounts);
- order a person to provide login information such as usernames and passwords, to gain access to a computer under investigation; and
- prevent a person from accessing a computer or account by changing a password or by other means.[117]

See also Response 20-21.

The **Computer Misuse and Cybersecurity Act** ("**CMCA**")[118] also involves personal data on computers. It is an offence to obtain, retain, supply, transmit or make available "personal information" obtained in violation of offences under the CMCA. [119] The definition of "personal information" would appear to involve personal data:

> 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 ... an individual, including ... biometric data, name, address, date of birth, national registration identity card number...[120]

See also Response 20-21.

Additionally, personal data located on computers may be affected by the **Cybersecurity Act**

[114] Advisory Guidelines for Selected Topics para 8.11.
[115] Advisory Guidelines for Selected Topics para 8.11.
[116] (Cap 68, 2012 Rev Ed). Available via Singapore Statutes Online. https://sso.agc.gov.sg. ("CPC"). The amendments were under the Criminal Justice Reform Bill (Bill No. 14/2018) ("CJRB") which was passed on March 19, 2018. Available via Singapore Statutes Online. https://sso.agc.gov.sg.
[117] CJRB c 9.
[118] (Cap 50A, 2007 Rev Ed). Available via Singapore Statutes Online. https://sso.agc.gov.sg. ("CMCA.")
[119] CMCA s 8A(1). Offences include: causing a computer to perform any function to secure unauthorized access to computer material (CMCA s 3); causing a computer to perform any function to secure access to computer material with intent to commit a CMCA offence (CMCA s 4); unauthorised modification of computer material (CMCA s 5); and unauthorised access, use or interception of computer services (CMCA s 6).
[120] CMCA s 8A(7).

("**Cybersecurity Act**").[121] Under this act, the relevant authorities may take measures with regard to computers and computer systems which are deemed "critical information infrastructure"[122] and/or affected by cybersecurity incidents,[123] including scanning the relevant computers for cybersecurity vulnerabilities.[124] See also Response 20-21.

The Commission only administers the PDPA; it does not administer the abovementioned statutes. Instead:

- the Criminal Procedure Code is administered by the Ministry of Law and related authorities;[125]
- the Computer Misuse and Cybersecurity Act is administered by the Ministry of Home Affairs;[126] and
- the Cybersecurity Act will be administered by the Ministry of Communications and Information and the Cyber Security Agency of Singapore.[127]

8. Is there any legislation and/or relevant case law covering the protection of personal data in the context of electronic communications for marketing purposes (please discriminate if it is a general legislation or case law, which also covers that context, or if it is a specific legislation or case law)?

9. In the event the previous answer is affirmative, please indicate the legislation and provide additional information:

9.1. Is there an opt-out system, an opt-in system or a third solution (please discriminate if different solutions for different data subjects or contexts are provided)?

9.2. Any additional/specific protection for the data subject in the context of electronic communications for marketing purposes.

Response 8-9

See the other Responses regarding the PDPA, which are also applicable to personal data protection in the context of electronic communications for marketing purposes.

IP addresses; cookies

If they can identify individuals, IP addresses and cookies may be considered personal data, and therefore subject to the PDPA.[128] However, there may not be a need to seek consent for the use of cookies to collect, use or disclose personal data where the individual involved is aware of

[121] No 9 of 2018. Available via Singapore Statutes Online. https://sso.agc.gov.sg. ("Cybersecurity Act"). The Act was passed on February 5, 2018. It replaces the CMCA on matters involving cybersecurity.
[122] Cybersecurity Act ss 7-16.
[123] Cybersecurity Act s 19.
[124] Cybersecurity Act s 20(2)(*b*)-(*f*).
[125] Singapore Parliamentary Debates, Official Report (19 March 2018) vol 94. Available via Parliament of Singapore. https://www.parliament.gov.sg.
[126] Singapore Parliamentary Debates, Official Report (3 April 2017) vol 94. Available via Parliament of Singapore. https://www.parliament.gov.sg.
[127] CSA Singapore: About Us. https://www.csa.gov.sg/about-us/our-organisation. Accessed 12 January 2018.
[128] Advisory Guidelines for Selected Topics paras 7.1-7.3, 7.6.

the purposes for such collection, use or disclosure and has voluntarily provided his personal data for such purposes (eg for transmitting personal data for effecting online communications, and storing information that the user enters in a web form to facilitate an online purchase).[129]

For activities that cannot take place without cookies, consent may be deemed if the individual voluntarily provides the personal data for that purpose of the activity and it is reasonable that he would do so.[130] "Consent may also be reflected in the way a user configures his interaction with the Internet", eg if he/she configures his browser "to accept certain cookies but rejects others."[131] However, an individual's failure to actively manage his/her browser settings does not imply consent to the collection, use and disclosure of his/her personal data by all websites for their stated purpose.[132]

The obligation to obtain consent lies with the organisation collecting such data (whether by itself or through data intermediaries).[133]

DNCR

The PDPA established a number of "Do Not Call Registries" (each a "DNCR")[134] to which a person may add (or remove) his Singapore **telephone number** (whether personal, business, or otherwise).[135] This is an opt-out system. No marketing messages shall be sent (whether in sound, text, visual or other form (including voice or video calls made through a data service or other electronic means))[136] to a Singapore telephone number which is in a relevant DNCR.[137] Even if a number is not in a DNCR, a marketing message sent to such number must include specific information on the sending individual or organisation,[138] and must not conceal the identity of the sender.[139]

No one shall, as a condition for supplying "goods, services, land, interest, or opportunity" (collectively "services"), require another to give consent for the sending of a marketing message to a Singapore phone number "beyond what is reasonable to provide" such services.[140] Consent given in such circumstances or obtained through providing false or misleading information or by using deceptive or misleading practices is not validly given.[141] Consent given

[129] Advisory Guidelines for Selected Topics para 7.8.
[130] Advisory Guidelines for Selected Topics para 7.8.
[131] Advisory Guidelines for Selected Topics para 7.9.
[132] Advisory Guidelines for Selected Topics para 7.9.
[133] Advisory Guidelines for Selected Topics para 7.10.
[134] PDPC (2017) Advisory Guidelines on the Do Not Call Provisions (para 1.8). https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/advisory-guidelines-on-the-dnc-provisions-(270717).pdf. Accessed 12 Jan 2018. ("Advisory Guidelines on DNCR Provisions.") The DNCR provisions came into effect on 2 January 2014: Personal Data Protection Act 2012 (Commencement) Notification 2013 (S 708 of 2013). Available via Singapore Statutes Online. https://sso.agc.gov.sg.
[135] PDPA ss 39-40; Advisory Guidelines on Key Concepts para 2.7.
[136] PDPA s 37; Advisory Guidelines on DNCR Provisions para 1.8.
[137] PDPA s 43(1). There are at present three DNCRs: for voice calls, text messages, and fax messages. Advisory Guidelines on DNCR Provisions para 1.8.
[138] PDPA s 44(1).
[139] PDPA s 45(1). This provision applies to voice calls only.
[140] PDPA s 46(1).
[141] PDPA s 46(2).

under the DNCR provisions may also be withdrawn at any time.[142]

The DNCR provisions apply where either the sender or recipient is in Singapore when the message is sent or accessed, respectively.[143] The DNCR provisions operate in conjunction with the rest of the PDPA, and organisations must comply with both sets of provisions regarding Singapore telephone numbers.[144]

Others

The Spam Control Act[145] governs unsolicited commercial communications sent in bulk via electronic mail. Concerning personal data, anyone who receives an unsubscribe request in connection with the sending of an unsolicited commercial electronic message shall not disclose any information contained in such request to any other person, except with the consent of the person whose particulars are contained in the unsubscribe request.[146]

As of 27 April 2018, the Commission is considering a merger of the DNC Provisions of the PDPA and the Spam Control Act under a single act governing "unsolicited commercial messages."[147] This follows similar approaches in jurisdictions such as Hong Kong and the United Kingdom.[148]

10. Is there any legislation and/or relevant case law regulating the processing of personal data of employees through electronic means (e.g., geolocation; CCTV cameras; performance monitoring; use of equipment, such as mobile phone; and professional electronic mail)? In case of an affirmative answer, please identify the legislation and/or relevant case law (please discriminate if it is a general legislation, which also covers that context, or if it is a specific legislation).

11. In the event the previous answer is affirmative, please provide additional information:

11.1. The type of processing of personal data regulated.

11.2. The processing of data permitted and the respective limitations (e.g., if the processing of data is limited to specific purposes or specific types of data).

Response 10-11

The PDPA applies to employees' personal data, irrespective of the form of the data.[149]

[142] PDPA s 47(6).
[143] PDPA s 38.
[144] Advisory Guidelines on Key Concepts para 2.7.
[145] (Cap 311A, 2008 Rev Ed). Available via Singapore Statutes Online. https://sso.agc.gov.sg. ("SCA.") The SCA is administered by the IMDA.
[146] SCA s 11 read with Second Schedule s 2(8).
[147] PDPC Factsheet. PDPC Proposes Combined Regime to Regulate Telemarketing and Spam Messages and Enhanced Guidance to Provide Regulatory Certainty (27 April 2018). https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Press-Room/2018/Factsheet-on-PDPA-Public-Consult-2-(270418).pdf. Accessed 19 June 2018. ("Combined Regime Proposal 2018")
[148] Combined Regime Proposal 2018.
[149] PDPC (2016) Protecting the Personal Data of Job Applicants and Employees (p 1). https://www.pdpc.gov.sg/resource/DPO-Connect/March-

Organisations should treat the personal data of their employees and job applicants "with equal care" and in the same manner as they would treat the personal data of any other individual.[150]

For instance, in *YesTuition Agency*,[151] the organisation (a tuition agency) disclosed on its website the national identification numbers and images of individuals who had registered to be tutors.[152] The Commission held that the organisation had breached the Consent Obligation by failing to obtain the tutors' consent for such disclosure.[153] And in *Jump Rope (Singapore)*,[154] the organisation sent an email to various schools notifying them of its blacklisting of the complainant, a former employee; the email included the complainant's name and national identification number. The Commission held that while there can be "valid business or legal reasons" for blacklisting a former employee, even if it requires disclosing his/her personal data, the organisation should at least have notified the former employee of such disclosure; such disclosure should also be "only for purposes that a reasonable person would consider appropriate in the circumstances."[155] In this case, not only was consent not obtained, but there was also no business or legal reason justifying said disclosure, eg if the complainant's post-employment conduct "had put the [organisation's] trade reputation or potential clients at risk."[156]

Exceptions. An organisation may collect, use or disclose employees' personal data without consent if the collection is "reasonable for the purpose of managing or terminating an employment relationship between the organisation and the individual" ("Managing/Terminating Purposes"),[157] or for evaluative purposes ("Evaluative Purposes");[158] or if the personal data was in a document "produced in the course, and for the purposes, of the [employee's] employment" and "collected for purposes consistent with the purposes for which the document was produced."[159]

Managing/Terminating Purposes include: "[u]sing the employee's bank account details to issue salaries"; "[m]onitoring how the employee uses company computer network resources"; "[p]osting employees' photographs on the staff directory page on the company intranet"; and "[m]anaging staff benefit schemes like training or educational subsidies."[160] Evaluative Purposes include obtaining performance records or other evaluative information to determine an employee's performance.[161]

The difference between the two purposes lies in the requirement to notify employees regarding

16/pdf/ProtectingthePersonalDataOfJobApplicants_and_Employees.pdf. Accessed 12 May 2017. ("Protecting the Personal Data of Job Applicants and Employees.")

[150] Protecting the Personal Data of Job Applicants and Employees p 1.

[151] [2016] SGPDPC 05.

[152] [2016] SGPDPC 05 at [1].

[153] [2016] SGPDPC 05 at [15].

[154] [2016] SGPDPC 21.

[155] [2016] SGPDPC 05 at [10].

[156] [2016] SGPDPC 05 at [12].

[157] PDPA Second Schedule s 1(*o*), Third Schedule s 1(*j*), Fourth Schedule s 1 (*s*).

[158] PDPA Second Schedule s 1(*f*), Third Schedule s 1(*f*), Fourth Schedule s 1(*h*).

[159] PDPA Second Schedule s 1(*n*), Third Schedule s 1(*j*), Fourth Schedule s 1(*s*).

[160] Advisory Guidelines for Selected Topics para 5.21.

[161] Advisory Guidelines for Selected Topics para 5.18.

actions for Managing/Terminating Purposes but not Evaluative Purposes.[162] An organisation shall, on or before collecting, using or disclosing personal data about an employee for Managing/Terminating Purposes, inform him/her of such purpose and (on request) provide the business contact information of a person who is able to answer the employee's questions about such collection, use or disclosure.[163] The manner of notification is not prescribed, but it may be appropriate to notify employees through avenues like "employment contracts, employee handbooks, or notices in the company intranet".[164] Organisations should also act based on what a reasonable person would consider appropriate in the circumstances.[165]

Organisations must still ensure that their employees' data is "properly protected, accurate and stored only for the period that it is needed."[166] Organisations must also allow the employee to access[167] and correct[168] his/her personal data, as well as withdraw consent.[169] Two important exceptions to an employer's Access Obligation are if: the data is solely for evaluative purposes;[170] and disclosing the data would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the organisation's competitive position.[171] There is also no need to correct personal data kept solely for evaluative purposes.[172]

CCTVs. The PDPA encompasses the use of CCTVs (at a workplace or otherwise), ie individuals must be informed of the purposes for which their personal data (obtained through the CCTV) will be collected, use or disclosed.[173] Additionally, notices should be placed "so as to enable individuals [including employees] to have sufficient awareness that CCTVs have been deployed for a particular purpose", eg at the entry to a building.[174] However, the exact location of the CCTV need not be revealed.[175] Concerning an access request for CCTV records, such access shall be provided unless an exception applies, eg if the records may reveal personal data about another individual.[176] (However, access can be given if the organisation masks the personal data of other individuals.)[177] A reasonable processing fee can also be charged.[178] The organisation may also reject access requests which are "frivolous or vexatious", or if the burden of providing access would be unreasonable to the organisation or disproportionate to the individual's interests.[179]

12. Is there any legislation or court decision giving orientation on the use of electronic

[162] Advisory Guidelines for Selected Topics para 5.24.
[163] PDPA s 20(4).
[164] Advisory Guidelines for Selected Topics para 5.20.
[165] Advisory Guidelines for Selected Topics para 5.26.
[166] PDPA s 23-25; Protecting the Personal Data of Job Applicants and Employees p 3.
[167] PDPA s 21.
[168] PDPA s 22.
[169] PDPA s 16(1). See Response 6-7 above.
[170] PDPA Fifth Schedule s 1(*a*).
[171] PDPA Fifth Schedule s 1(*g*).
[172] PDPA Sixth Schedule s 1(*a*).
[173] Advisory Guidelines for Selected Topics para 4.34.
[174] Advisory Guidelines for Selected Topics para 4.36.
[175] Advisory Guidelines for Selected Topics para 4.38.
[176] Advisory Guidelines for Selected Topics para 4.42-4.43 (discussing PDPA s 21(3)(*c*)).
[177] Advisory Guidelines for Selected Topics para 4.43(c).
[178] PDPR s 7; Advisory Guidelines for Selected Topics para 4.46.
[179] PDPA s 21(2) read with Fifth Schedule s 1(*j*)(ii), (v).

means by the employees and, in particular, is there any legislation or court decision giving orientation on the nature of the information (public or private information) shared by employees through social networks and on the possibility to use it as evidence within disciplinary proceedings?

Response 12

There is no specific legislation or case law on this point. However, in *My Digital Lock Pte Ltd*,[180] the complainant and respondent were engaged in a legal dispute. Respondent's director "A" posted screenshots of the complainant's WhatsApp conversations with A (which included the complainant's personal mobile phone number and residential address) on A's Facebook page.[181] A claimed he merely intended to transfer the screenshots to his lawyers.[182] The Commission held that the transfer over Facebook "was wholly inappropriate" and unreasonable, and there "were other ways" to send the screenshots.[183] A could have encrypted or password protected the screenshots, or even "connected his phone to his PC and transferred the file without ... mak[ing] use of the open Internet."[184] As A was acting in the course of his employment with respondent, the respondent failed to make reasonable security arrangements to protect personal data in its possession or control, and was in breach of the PDPA.[185]

Additionally, employees who post material on social networks could be subject to defamation claims, both criminal[186] and civil[187], as well as claims of malicious falsehood.[188] Other claims could include breach of confidence (eg through the unauthorised posting of private information)[189] and copyright infringement (eg by posting materials to which the poster does not have the copyright).[190] Employees have also been simply fired for unwise postings on social media.[191]

Vicarious liability may also apply if such employees' actions could be attributed to the

[180] [2016] SGPDPC 20.
[181] [2016] SGPDPC 20 at [4], [13].
[182] [2016] SGPDPC 20 at [21].
[183] [2016] SGPDPC 20 at [21], [25].
[184] [2016] SGPDPC 20 at [25].
[185] [2016] SGPDPC 20 at [14], [24]-[26].
[186] Penal Code (Cap 224, 200 Rev Ed) s 499.
[187] See, eg, *Golden Season Pte Ltd v Kairos Singapore Holdings Pte Ltd* [2015] SGHC 38 (involving claims of defamation and malicious falsehood through an employee's statements regarding another entity, made via Facebook, emails and text messages).
[188] See *Golden Season Pte Ltd v Kairos Singapore Holdings Pte Ltd* [2015] SGHC 38.
[189] See Chan paras 16.020-16.027.
[190] See *Golden Season Pte Ltd v Kairos Singapore Holdings Pte Ltd* [2015] SGHC 38. See also Tan B (2011) Social Media in the Workplace: Challenges and Implications. http://www.lawgazette.com.sg/2011-06/131.htm. Accessed 15 May 2017; Sedition Act (Cap 290, 2013 Rev Ed); Public Order Act (Chapter 257A); and the Penal Code (Cap 224, 2008 Rev Ed).
[191] See, eg, Linette Lai (2016) Aussie expat fired after offensive Facebook rant. In: The Straits Times http://www.straitstimes.com/singapore/aussie-expat-fired-after-offensive-facebook-rant. Accessed 11 May 2017.

employer, whether under the PDPA[192] or other law.[193]

13. Are there any additional/specific obligations in order to protect personal data conveyed and stored through electronic means?

Response 13

The PDPA states that an organisation "shall protect personal data in its possession or ... control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks."[194] The Commission's guidelines reiterate the need to adopt arrangements which are reasonable under the circumstances.[195]

For instance, an organisation should ensure that its security arrangements "fit the nature of the personal data held ... and the possible harm that might result from a security breach"; "identify reliable and well-trained personnel"; "implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity"; and "be prepared and able to respond to information security breaches promptly and effectively."[196] Thus in *My Digital Lock Pte Ltd*,[197] the Commission stated that "[r]easonable ... security arrangements when transferring personal data" requires a process where "the personal data is reasonably protected from unauthorised access or interference, until the personal data reaches its intended destination or recipient where other security arrangements on storage would apply."

Guidelines have also been issued in this regard, concerning: the security and protection of personal data stored in electronic medium; good practices for protecting electronic personal data; and enhanced practices that may be adopted.[198] For instance, organisations should ensure that computer networks are secure, and personal data encrypted.[199] They should consider, as part of good governance: accountability; standards, policies and procedures; risk management; and classification and tracking of personal data.[200] They should also educate employees on potential threats to, and protection measures for, personal data.[201]

There are also guidelines on preventing accidental disclosure of personal data, including: automating the processing of documents containing personal data and checking these systems regularly; ensuring additional checks following the processing, printing and sorting of documents to ensure that the destination information is correct and matches that of the intended recipient; and establishing a policy for sending compiled sets of personal data of different

[192] PDPA s 53(1).
[193] See Chan paras 19.001 *et seq*.
[194] PDPA s 24.
[195] Advisory Guidelines on Key Concepts para 17.2.
[196] Advisory Guidelines on Key Concepts para 17.3.
[197] [2016] SGPDPC 20 at [25].
[198] PDPC (2016) Guide to Securing Personal Data in Electronic Medium (para 2.3). https://www.pdpc.gov.sg/docs/default-source/other-guides/guide-to-securing-personal-data-in-electronic-medium-(200117).pdf. Accessed 12 May 2017. ("Guide to Securing Personal Data in Electronic Medium.")
[199] Guide to Securing Personal Data in Electronic Medium paras 9.1, 10.3.
[200] Guide to Securing Personal Data in Electronic Medium para 4.1.
[201] Guide to Securing Personal Data in Electronic Medium paras 5.1-5.2.

individuals (eg through spreadsheets).[202] The use of passwords for documents containing personal data, as well as regular staff training on proper data protection procedures, is also encouraged.[203]

These guidelines reflect the approach taken in several cases decided by the Commission. For instance, in *The Institution of Engineers Singapore*[204] ("IES"), there was a breach of personal data of IES members stored on the organisation's website. While a number of measures had been taken to secure the site, including use of a firewall and anti-virus software, up-to-date software, and limited administrative access, the Commission found the following flaws: no encrypted storage of member passwords; no security audit on the website; no penetrating testing; and no specific arrangements with the website vendors to put in place security measures to safeguard personal data stored on the website.[205] In addition, there were common vulnerabilities with the website (including cross-site scripting); these could have been easily detected through the performance of a vulnerability scan, which was also an industry best practice.[206]

And in *Central Depository (Pte) Limited*[207] ("CDP"), the external vendor hired by CDP to print member account statements was found to have breached the PDPA, through sending out six member account statements that contained account information of other account holders. Due to errors in the sorting and compilation process, the first page of the statement of an account holder was compiled with the second and subsequent pages of another account holder.[208] A vendor employee had marked out the errors, telling another employee to discard the incorrect statements and replace them with the correct ones.[209] Unfortunately, that second employee "mistakenly discarded the correct statements" and mailed out the incorrect statements instead.[210] The Commission held that the errors "could have been avoided by putting in place processes or technology solutions that can minimise human error."[211]

Based on caselaw, factors that the Commission has taken into account regarding reasonable protection of personal data conveyed and stored through electronic means include:[212] failure to audit systems, carry out penetration tests and test website vulnerabilities;[213] use of outdated

---

[202] PDPC (2017) Guide to Preventing Accidental Disclosure when Processing and Sending Personal Data (pp 3-4). https://www.pdpc.gov.sg/docs/default-source/other-guides/guide-to-preventing-accidental-disclosure-when-processing-and-sending-personal-data-(200117).pdf. Accessed 12 May 2017. ("Guide to Preventing Accidental Disclosure.")
[203] Guide to Preventing Accidental Disclosure p 5.
[204] [2016] SGPDPC 02.
[205] [2016] SGPDPC 02 at [29]-[30], [33].
[206] [2016] SGPDPC 02 at [31]-[32].
[207] [2016] SGPDPC 11.
[208] [2016] SGPDPC 11 at [7].
[209] [2016] SGPDPC 11 at [7].
[210] [2016] SGPDPC 11 at [7].
[211] [2016] SGPDPC 11 at [20].
[212] Woon CY (2016) Personal Data Protection Act – Obligation to Protect and Secure Data, and What to do in case of Breach. https://dentons.rodyk.com/en/insights/alerts/2016/november/8/personal-data-protection-act-obligations-to-protect-and-secure-data-and-what-to-do-in-case-of-breach. Accessed 12 May 2017.
[213][213] See *K Box Entertainment Group Pte. Ltd.* [2016] SGPDPC 01.

software and/or failure to recognise vulnerabilities associated with software or hardware;[214] failure to address common website vulnerabilities such as SQL injection vulnerabilities[215] and cross-site scripting;[216] use of the auto-fill function;[217] failure to remove unused user accounts or limit access to website administration;[218] and failure to use encryption and/or strong passwords (or any passwords at all).[219]
Other factors (which seem equally applicable to non-electronic data breaches) include: whether personal data was in fact disclosed and, if so, the number of individuals whose personal data was disclosed[220] and the sensitivity of the data involved;[221] and failure to implement adequate data protection procedures and policies (including appointing a data protection officer).[222] Finally, the Commission also considers whether: prompt remedial action was taken;[223] the affected parties were notified of the breach;[224] and if the organisation was cooperative and forthcoming during the Commission's investigations.[225]

Limited Retention
Organisations must cease retaining personal data as soon as it is "reasonable" to assume that the purpose for which the personal data was collected is no longer served by such retention, and retention is no longer necessary for legal or business purposes.[226] Thus, an organisation may not retain data "just in case" the data may be needed for other purposes.[227]

---

[214] See *K Box Entertainment Group Pte. Ltd.* [2016] SGPDPC 01; *Institution of Engineers* [2016] SGPDPC 02.
[215] See *Metro Pte Ltd* [2016] SGPDPC 07.
[216] See *Institution of Engineers* [2016] SGPDPC 02.
[217] See *Full House Communications Pte Ltd* [2016] SGPDPC 08.
[218] See *K Box Entertainment Group Pte. Ltd.* [2016] SGPDPC 01; *Fei Fah Medical Manufacturing Pte. Ltd.* [2016] SGPDPC 03.
[219] See *K Box Entertainment Group Pte. Ltd.* [2016] SGPDPC 01; *Institution of Engineers* [2016] SGPDPC 02; *My Digital Lock Pte Ltd* [2016] SGPDPC 20; *Fu Kwee Kitchen Catering Services* [2016] SGPDPC 14; *Smiling Orchid* [2016] SGPDPC 19; *The Cellar Door Pte Ltd* [2016] SGPDPC 22.
[220] See *K Box Entertainment Group Pte. Ltd.* [2016] SGPDPC 01; *Institution of Engineers* [2016] SGPDPC 02; *Aviva Ltd* [2016] SGPDPC 15; *Comfort Transportation Pte Ltd* [2016] SGPDPC 17.
[221] See *Aviva Ltd* [2016] SGPDPC 15; *Central Depository (Pte) Limited* [2016] SGPDPC 11; *Challenger Technologies Limited* [2016] SGPDPC 06.
[222] See, eg, *K Box Entertainment Group Pte. Ltd.* [2016] SGPDPC 01; *Fu Kwee Kitchen Catering Services* [2016] SGPDPC 14; *National University of Singapore* [2017] SGPDPC 05; *Tiger Airways Singapore Pte Ltd SATS Ltd Asia-Pacific Star Private Limited* [2017] SGPDPC 06; *M Stars Movers & Logistics Specialist Pte Ltd* [2017] SGPDPC 15.
[223] See *Central Depository (Pte) Limited* [2016] SGPDPC 11; *Challenger Technologies Limited* [2016] SGPDPC 06; Spear Security Force Pte. Ltd. [2016] SGPDPC 12; ABR Holdings Limited [2016] SGPDPC 16.
[224] See *Institution of Engineers* [2016] SGPDPC 02;
[225] See *Institution of Engineers* [2016] SGPDPC 02; *Fei Fah Medical Manufacturing Pte. Ltd.* [2016] SGPDPC 03; *YesTuition Agency* [2016] SGPDPC 05; *Singapore Computer Society* [2016] SGPDPC 09; *Central Depository (Pte) Limited* [2016] SGPDPC 11.
[226] PDPA s 25.
[227] Advisory Guidelines on Key Concepts para 18.4.

An organisation ceases to retain documents containing personal data when it, its agents and its data intermediaries no longer have access to those documents and the personal data they contain, eg by destroying the documents or anonymising the data.[228] Documents should be "completely irretrievable or inaccessible" to the organisation.[229] Data in electronic form which is archived or to which access is limited is still considered retained.[230]

Factors to consider in determining whether an organisation has ceased to retain personal data are: whether the organisation has any intention to use or access the personal data; the effort and resources needed to use or access the personal data again; whether third parties have been given access to that personal data; and whether the organisation has made a reasonable attempt to destroy, dispose of or delete the personal data in a permanent and complete manner.[231]

Data intermediaries

A data intermediary is "an organisation which processes personal data on behalf of another organisation."[232] A data intermediary has no obligation under the PDPA save for the Protection Obligation and the Retention Obligation.[233] Such Obligations may also apply to data intermediaries who are overseas.[234]

Instead, an organisation who uses a data intermediary shall have the same obligation in respect of personal data processed on its behalf by a data intermediary as if the data were processed by the organisation itself.[235] Indeed, it has been said that "Singapore has enacted a form of vicarious liability on Singaporean data controllers for overseas processing."[236]

PS(G)A

Data shared under the PS(G)A will be "for analysis and to develop policies and programmes".[237] Such data will be anonymised and aggregated.[238] As such, "centralised data custodians" will be set up where "raw data from different sources will be matched and anonymised, before being released to relevant agencies for analysis."[239] Moreover, the user of the data will also be held "accountable for the protection and safeguarding of data passed to" it.[240] Unauthorised disclosure and improper use of information shared under the PS(G)A will

---

[228] Advisory Guidelines on Key Concepts para 18.10.
[229] Advisory Guidelines on Key Concepts para 18.12.
[230] Advisory Guidelines on Key Concepts para 18.11.
[231] Advisory Guidelines on Key Concepts para 18.13. See, eg, *Orchard Turn Developments Pte. Ltd.* [2017] SGPDPC 12 (failure to purge personal data from server led to data breach; retention of data was also unnecessary); *Social Metric Pte Ltd* [2017] SGPDPC 17 (company penalized for, in part, failure to cease retaining personal data).
[232] PDPA s 2(1).
[233] PDPA s 4(2). See, eg, *K Box Entertainment Group Pte. Ltd.* [2016] SGPDPC 01; *Challenger Technologies Limited* [2016] SGPDPC 06.
[234] Greenleaf, G (2014) Comparisons with Other Asian Jurisdictions (para 8.55). In: Chesterman, S (ed) Data protection law in Singapore: privacy and sovereignty in an interconnected world. Academy Publishing, Singapore. ("Greenleaf.")
[235] PDPA s 4(3).
[236] Greenleaf para 8.55.
[237] Singapore Parliamentary Debates, Official Report (8 January 2018) vol 94.
[238] Singapore Parliamentary Debates, Official Report (8 January 2018) vol 94.
[239] Singapore Parliamentary Debates, Official Report (8 January 2018) vol 94.
[240] Singapore Parliamentary Debates, Official Report (8 January 2018) vol 94.

be punished,[241] as will "unauthorised re-identification of anonymised information".[242] Public servants' access to data will also be prescribed based on security clearance and legitimate need.[243]

14. Is there an obligation to inform any third party or the data subject about data breaches or incidents concerning the security of personal data processed by electronic means and, in case of an affirmative response, what are the presuppositions for such an obligation?

Response 14

Singapore intends to adopt a mandatory data breach notification regime.[244] Relevant legislation is intended to be tabled in Parliament in 2019.[245] Under this change:[246]

- where a data breach is "likely to result in significant harm or impact to the individuals to whom the information relates", the organisation must notify both (a) the individuals affected and (b) the Commission of the breach; and
- where the scale of the breach is "significant", the organisation must notify the Commission of the breach, even if the breach does not pose any risk of impact or harm to the affected individuals.

The organisation will have up to 30 days to assess the suspected breach.[247] If the organisation decides that the breach is eligible for reporting, the organisation must notify (a) affected individuals of the breach "as soon as practicable" from the time it determines the breach is eligible for reporting, and (b) the Commission within 72 hours of such time.[248]

The organisation will not have to notify affected individuals of:[249]

- an eligible breach which is the subject of an ongoing or potential investigation under the law, if such notification will compromise investigations or prejudice enforcement efforts ("law-enforcement exception");
- a breach of data which has been encrypted to a reasonable standard, unless the data can be decrypted ("technological protection exception"); and/or
- an eligible breach if the organisation has taken actions to reduce the potential harm or impact to affected individuals, if the organisation demonstrates that as a result of its actions the breach is not likely to have any significant harm or impact to such individuals.

However, regardless of these exceptions, organisations will still have to notify the Commission

[241] PS(G)A s7.
[242] PS(G)A s8.
[243] Singapore Parliamentary Debates, Official Report (8 January 2018) vol 94; New law on data sharing among govt agencies <http://www.straitstimes.com/singapore/new-law-on-data-sharing-among-govt-agencies> January 9, 2018.
[244] Public Consultation June 2018 (Part III).
[245] "Breach reporting part of revised data privacy laws to be tabled in Parliament" https://www.straitstimes.com/tech/breach-reporting-part-of-revised-data-privacy-laws-to-be-tabled-in-parliament (February 1, 2018). Accessed 7 June 2018.
[246] Public Consultation June 2018 (paras 8.4-8.5).
[247] Public Consultation June 2018 (para 9.5).
[248] Public Consultation June 2018 (paras 9.4-9.7).
[249] Public Consultation June 2018 (paras 10.4-10.8).

of an eligible breach.[250] Finally, where an organisation is required to notify another agency of a data breach under other written law, such notification must take place in accordance with such other law.[251]

15. Is there any specific legislation or relevant self-regulation instruments on sectorial areas regarding the processing of personal data by electronic means (e.g., homebanking, unmanned aerial vehicles/mobile health/IoT)? In case of an affirmative answer, please identify and briefly elaborate on those specific rules.

Response 15

See Response 16-17 regarding legislation on personal data processing in the electronic communications sector. The Commission has also issued guidelines regarding the protection of personal data for the healthcare,[252] education,[253] social services,[254] and real estate[255] sectors. Generally, these guidelines discuss the general provisions of the PDPA, as applied to possible scenarios which could arise in that particular sector.

Additionally, the Monetary Authority of Singapore ("MAS") has issued Technology Risk Management Guidelines[256] which are applicable to, among others, banks, finance companies and institutions, insurance companies, financial advisers, and financial holding companies. It provides comprehensive guidelines for securing, both physically and online, the institutions' computer systems, networks, data centers, operations and backup facilities.

Specifically, "(e)ffective risk management practices and internal controls should be instituted to achieve", among others, data confidentiality, meaning "the protection of sensitive or confidential information such as customer data from unauthorised access, disclosure, etc."[257] Institutions shall also implement (or ensure that service providers implement) procedures and

[250] Public Consultation June 2018 (para 10.7).
[251] Public Consultation June 2018 (para 11.3).
[252] PDPC (2017) Advisory Guidelines for the Healthcare Sector. https://www.pdpc.gov.sg/docs/default-source/public-consultation-4---education-healthcare-social-services-photography-submissions/advisory-guidelines-for-the-healthcare-sector-(28-mar-2017).pdf. Accessed 12 May 2017.
[253] PDPC (2014) Advisory Guidelines for the Education Sector. https://www.pdpc.gov.sg/docs/default-source/public-consultation-4---education-healthcare-social-services-photography-submissions/advisory-guidelines-for-the-education-sector.pdf. Accessed 12 May 2017.
[254] PDPC (2014) Advisory Guidelines for the Social Service Sector. https://www.pdpc.gov.sg/docs/default-source/public-consultation-4---education-healthcare-social-services-photography-submissions/advisory-guidelines-for-the-social-services-sector.pdf. 12 May 2017.
[255] PDPC (2014) Advisory Guidelines for the Real Estate Agency Sector. https://www.pdpc.gov.sg/docs/default-source/public-consultation-3-(real-estate-telecomm)-submissions-/real-estate.pdf. Accessed 12 May 2017.
[256] MAS (2013) Technology Risk Management Guidelines. http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf. Accessed 12 May 2017. ("TRMG.")
[257] TRMG para 4.0.2.

"to protect the confidentiality and security of its sensitive or confidential information, such as customer data."[258] Institutions should also "keep customers informed of any major incident" and informing the general public "where necessary."[259] While the TRMG are "not legally binding, the degree of observance with the spirit of the [g]uidelines … is an area of consideration in the risk assessment of the [institution] by MAS."[260]

Other regulatory agencies may work with the Commission with regard to data protection breaches. For instance, MAS stated that "in cases involving disclosure of banking customers' personal data," it would work with the Commission "to review the matter."[261]

Various industries, such as the Life Insurance Association Singapore ("LIA")[262] and The Association of Banks in Singapore ("ABS")[263] have also issued codes of conduct regarding personal data protection.

III. DATA PROTECTION IN THE ELECTRONIC COMMUNICATIONS SECTOR

16. Is there any specific legal rules and/or relevant case law regarding the processing of personal data in the electronic communications sector? In case the answer is affirmative, please identify the applicable legislation and/or relevant case law (please discriminate if it is a general legislation or case law, which also covers that context, or if it is a specific legislation or case law).

17. In the event the previous answer is affirmative, please provide additional information:

17.1. Please indicate the entities subject to these legal rules or relevant case law (e.g., public communications networks providers and/or publicly available electronic communications services providers)?

17.2. What does "communication data" mean in the legislation and/or case law? In case different meanings result from different legislation, please specify each one of

[258] TRMG para 5.1.4.
[259] TRMG para 7.3.9.
[260] TRMG para 1.0.5.
[261] This was in reference to an incident where reporters found, in a public area, a trashbag containing "several corporate statements, loan applications, and internal reports from [a] bank." Lee J (2016) MAS probes case of UOB's unshredded client data. In: The Straits Times. http://www.straitstimes.com/business/companies-markets/mas-probes-case-of-uobs-unshredded-client-data. Accessed 12 May 2017. The outcome of the investigation remains unclear: Koh WT (2016) UOB under MAS probe for failing to protect clients' privacy. In: The Straits Times. http://themiddleground.sg/2016/07/19/uob-mas-probe-failing-protect-client-privacy. Accessed 12 May 2017.
[262] Life Insurance Association Singapore (2015) MU61/15 – LIA Code of Practice for Life Insurers on the Singapore Personal Data Protection Act (No. 26 of 2012). http://www.lia.org.sg/node/4132. Accessed 12 May 2017. Life Insurance Association Singapore (2015) MU 62/15 - LIA Code Of Conduct For Tied Agents Of Life Insurers On The Singapore Personal Data Protection Act (No. 26 of 2012). http://www.lia.org.sg/node/4133. Accessed 12 May 2017.
[263] The Association of Banks in Singapore (2015) Code of Banking Practices – The Personal Data Protection Act ("PDPA"). https://abs.org.sg/docs/library/abs-code-banking-practices-pdpa.pdf. Accessed 12 May 2017.

them.
17.3. Is "communication data" classified in categories in the legislation and/or case law? In case of an affirmative answer, please indicate the categories.
17.4. Please indicate specific legal rules, if any, about the confidentiality of communication data.
17.5. Please indicate specific legal rules, if any, about the implementation of security measures by the electronic communications providers in order to protect personal data, and obligations in case of risk of a breach of the security.
17.6. Please indicate specific legal rules, if any, about data breaches, including any obligations to notify the data subject, a supervisory body or any other third party in case a data breach occurs.

Response 16-17

The PDPA applies generally to the electronic communications sector as well. See the other Responses.

The Commission's guidelines also provide some examples of the PDPA as applied to the telecommunications sector.[264] For instance, the guidelines discuss what may constitute "personal data" in the telecommunications context: eg an individual's mobile telephone number and, if combined with other information, an Internet Protocol ("IP") address and International Mobile Equipment Identity ("IMEI") numbers.[265]

- Thus, when a Singapore telecommunications operator provider exchanges personal data with a foreign telecommunication operator to allow the latter to provide mobile services to outbound roamers who are subscribers of the Singapore operator, the Singapore operator will need to comply with the Notification, Consent and Limited Transfer Obligations, as discussed in Responses 6-7 and 28.[266]

In addition, the **Telecommunications Act**[267] and the **Electronic Transactions Act (ETA)**[268] (both also administered by the IMDA) touch on certain aspects of personal data protection.

Under the Telecommunications Act, a public telecommunication licensee has no liability to anyone due to "any loss of secrecy in communication arising from the use of any telecommunication service" due to "the act or default of another person, or an accident or some other cause" beyond the licensee's control.[269] More specifically with regard to personal data, the act also "sets out certain purposes for which telecommunication operator[s] may collect, use or disclose End User Service Information ["EUSI"], some of which qualify as personal

[264] PDPC (2014) Advisory Guidelines for the Telecommunication Sector. https://www.pdpc.gov.sg/docs/default-source/public-consultation-3-(real-estate-telecomm)-submissions-/finalised-advisory-guidelines-on-application-of-pdpa-to-telecom-sector.pdf. Accessed 13 May 2017. ("Advisory Guidelines for the Telecommunication Sector.")
[265] Advisory Guidelines for the Telecommunication Sector paras 2.4-2.5.
[266] Advisory Guidelines for the Telecommunication Sector para 3.7.
[267] (Cap 323, 2000 Rev Ed). Available via Singapore Statutes Online. https://sso.agc.gov.sg. ("Telecommunications Act.")
[268] (Cap 88, 2011 Rev Ed). Available via Singapore Statutes Online. https://sso.agc.gov.sg. ("ETA.")
[269] Telecommunications Act s 70(*d*).

data, without consent,"[270] including "collection or use of [a] Residential End User's EUSI as ... reasonably necessary for planning requirements in relation to network operations or network maintenance" and "collection, use or disclosure of Residential End User's EUSI as ... reasonably necessary for facilitating interconnection and interoperability ... for the provision of Services." [271] Additionally, regarding the DNCR provisions in the PDPA, a "telecommunications service provider who merely provides a service" that enables a message to be sent shall "be presumed not to have sent the message and not to have authorised the message to be sent."[272]

The ETA defines "electronic communication" as "any communication that the parties make by means of electronic records", meaning "a record generated, communicated, received or stored by electronic means in an information system or for transmission from one information system to another".[273]

Concerning personal data: pursuant to the enactment of the PDPA, the ETA was specifically amended to state that an NSP "shall not be subject to any liability" under the PDPA "in respect of third-party material in the form of electronic records to which [it] merely provides access,"[274] including the "temporary and automatic caching of third party material in the form of electronic records (that contains personal data) ... provided that such caching is ... for the purpose of ... merely providing access to the third party material."[275]

18. Please indicate any supervising body in charge of the control of the processing of personal data in the context of electronic communications, if any.

19. In the event there is a supervisory body specific for the electronic communications context, please indicate the main types of powers vested in this supervisory body, including sanctioning powers.

Response 18-19

See Response 3-4.

Under the Telecommunications Act, IMDA shall operate and provide telecommunication systems and services in Singapore, with the power to impose penalties for violations of the act, including suspending or cancelling telecommunications licenses.[276] It may also conduct investigations under the act, including arresting certain wrongdoers thereunder.[277]

[270] Advisory Guidelines for the Telecommunication Sector para 4.3.
[271] IMDA (2014) Code Of Practice For Competition In The Provision Of Telecommunication Services 2012 (para 3.2.6.2). <https://www.imda.gov.sg/~/media/imda/files/regulation%20licensing%20and%20consultations/frameworks%20and%20policies/competition%20management/telecom%20competition%20code/02%202012tccwef2july2014.pdf?la=en>. Accessed 12 May 2017.
[272] PDPA s 36(2).
[273] ETA s 2(1).
[274] Personal Data Protection Bill (No 24 of 2012) s 67(2). Available via Singapore Statutes Online. https://sso.agc.gov.sg; ETA s 26(1A).
[275] Advisory Guidelines for the Telecommunication Sector para 4.2.
[276] See, eg, Telecommunications Act Part II.
[277] Telecommunications Act Part VIII.

Under the ETA, IMDA shall, among others, facilitate communications through reliable electronic records; promote confidence in the integrity and reliability of electronic commerce; and implement the United Nations Convention on the Use of Electronic Communications in International Contracts adopted by the General Assembly of the United Nations on 23rd November 2005.[278] IMDA may conduct investigations under the ETA,[279] and compound any offences under the act.[280]

IV. DATA PROTECTION AND DIGITAL FORENSICS

20. Are there any exceptions/restrictions or, in any way, specific rules applicable to the protection of personal data for the purpose of the investigation, detection and prosecution of crimes through electronic means? In case the answer is affirmative, please identify the applicable legislation and/or relevant case law (please discriminate if it is a general legislation or case law, which also covers that context, or if it is a specific legislation or case law).

21. In the event the previous answer is affirmative, please provide additional information:

21.1. Preservation and access to computer data hosted on a computer system

(i) Is there any legislation regarding the preservation, handling and/or access to computer data hosted on a computer system for the purpose of the investigation, detection and prosecution of crimes?

(ii) In case the previous answer is affirmative, what are the requirements (objective - e.g., type of crimes – subjective from the perspective of the authorities – e.g., judicial mandate, police order -, subjective from the perspective of the data subjects covered – e.g., suspect, victims – and others - e.g., the time limit, the procedures)?

21.2. Interception of communication data

(i) Is there any legislation regarding the interception of communication data for the purpose of the investigation, detection and prosecution of crimes?

(ii) In case the previous answer is affirmative, what is the permitted scope (e.g., content data, traffic data, location data)?

(iii)In case the answer in (i) is affirmative, what are the requirements (objective - e.g., type of crimes – subjective from the perspective of the authorities – e.g., judicial mandate, police order -, subjective from the perspective of the data subjects covered – e.g., suspect, victims – and others - e.g., the time limit, the procedures)?

21.3. Data retention

(i) Is there any legislation regarding data retention for the purpose of the investigation, detection and prosecution of crimes?

(ii) In case the previous answer is affirmative, what is the permitted scope (e.g., traffic data, location data)?

(iii) In case the answer in (i) is affirmative, what are the requirements (objective - e.g., type of crimes – subjective from the perspective of the

[278] ETA s 3.
[279] ETA s 24.
[280] ETA s 36(1).

	authorities – e.g., judicial mandate, police order -, subjective from the perspective of the data subjects covered - e.g., suspect, victims - and others - e.g., the time limit, the procedures)?

Response 20-21

The PDPA provides various exceptions from the various Obligations due to criminal investigations:[281]

- Collection without consent is allowed if it "is necessary for any investigation or proceedings, if it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data;"[282]
- Use and disclosure without consent is allowed if such use or disclosure "is necessary for any investigation or proceedings"[283] or disclosed to an officer of a law enforcement agency;[284]
- Access is not required for: "a document related to a prosecution if all proceedings related to the prosecution have not been completed"; personal data "subject to legal privilege"; or personal data collected, used or disclosed without consent for an investigation (pursuant to the consent exceptions in Second, Third and Fourth Schedules regarding investigations) if "the investigation and associated proceedings and appeals have not been completed";[285] additionally, an organisation shall not inform an individual that it has disclosed personal data to a law enforcement agency, if such disclosure was made without that individual's consent (pursuant to the Fourth Schedule or other law);[286] and
- Correction is not required for a document related to a prosecution "if all proceedings related to the prosecution have not been completed."[287]

More generally, pursuant to an investigation the police may access and inspect computers (including computer networks), as well as decrypt data on computers and networks.[288] For instance, under the recent amendments to the **Criminal Procedure Code**, investigators will be able to:

- Inspect and search any data stored on or available to a computer implicated in the investigation, regardless of whether the computer is inside or outside Singapore (thus this could include web-based email accounts and web storage accounts);
- order a person to provide login information such as usernames and passwords, to gain access to a computer under investigation; and
- prevent a person from accessing a computer or account by changing a password or by other means.[289]

The **CMCA** also involves personal data on computers. It is an offence to obtain, retain, supply,

[281] PDPA s 2(1).
[282] PDPA Second Schedule s 1(*e*).
[283] PDPA Third Schedule s 1(*e*), Fourth Schedule s 1(*f*).
[284] PDPA Fourth Schedule s 1(*n*).
[285] PDPA Fifth Schedule s 1(*e*), (*f*), (*h*).
[286] PDPA s 21(4).
[287] PDPA Sixth Schedule 1(*e*).
[288] Criminal Procedure Code (Cap 68, 2012 Rev Ed) s 39-40, read with CMCA s 2(1). Available via Singapore Statutes Online. https://sso.agc.gov.sg.
[289] CJRB c 9.

transmit or make available "personal information" obtained in violation of offences under the CMCA.[290] The definition of "personal information" would appear to involve personal data:

> 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 ... an individual, including ... biometric data, name, address, date of birth, national registration identity card number...[291]

Under the **Cybersecurity Act**, the Commissioner of Cybersecurity may require information concerning a computer or computer system (including any data therein) to determine if it is a "critical information infrastructure" ("CII").[292] If there is a cybersecurity incident, the Commissioner may also take investigatory steps, including: scanning the computer(s), preserving the computer(s) by not using it, taking extracts from any electronic record or computer program in the computer(s), and (with the owner's consent) taking possession of the computer(s).[293]

V. DATA PROTECTION AND ELECTRONIC SURVEILLANCE FOR SECURITY AND DEFENCE PURPOSES

22. Is there any legislation and/or relevant case law regarding the electronic processing of personal data for security and national defence purposes? In case the answer is affirmative, please identify the applicable legislation and/or relevant case law (please discriminate if it is a general legislation or case law, which also covers that context, or if it is a specific legislation or case law).

23. In case the previous answer is affirmative, please provide additional information:
23.1. What is the permitted scope (purposes covered – e.g., direct threats to national defence - type of activities permitted – e.g., preservation and access to computer data hosted on a computer system, interception of communication data, data retention or others – and categories of data covered – e.g., content data, traffic data, location data)?
23.2. What are the requirements (objective - e.g., type of threats covered – subjective from the perspective of the authorities – e.g., judicial mandate, police order-, subjective from the perspective of the data subjects covered - e.g., suspect, probable victims, civil, military, citizens, foreign entities - and others - e.g., the time limit, the procedures)?

Response 22-23

A number of statutes discuss the electronic processing of personal data for security and national defence purposes.

[290] CMCA s 8A(1). Offences include: causing a computer to perform any function to secure unauthorized access to computer material (CMCA s 3); causing a computer to perform any function to secure access to computer material with intent to commit a CMCA offence (CMCA s 4); unauthorised modification of computer material (CMCA s 5); and unauthorised access, use or interception of computer services (CMCA s 6).
[291] CMCA s 8A(7).
[292] Cybersecurity Act s 8.
[293] Cybersecurity Act s 20.

First, under the **PDPA**, an organisation shall not provide an individual with his/her personal data (or information about the ways in which the data has or may have been used or disclosed by the organisation) if the provision of that data or other information could reasonably be expected to "be contrary to the national interest".[294] Additionally, consent is not required for the collection, use or disclosure of personal data where such collection, use or disclosure is in the national interest.[295] National interest includes "national defence, national security, public security, the maintenance of essential services and the conduct of international affairs".[296]

Second, under recent amendments to the **Criminal Procedure Code**, investigators will be able to:

- Inspect and search any data stored on or available to a computer implicated in the investigation, regardless of whether the computer is inside or outside Singapore (thus this could include web-based email accounts and web storage accounts);
- order a person to provide login information such as username and password, to gain access to a computer under investigation; and
- prevent a person from accessing a computer or account by changing its password or by other means.

Third, the **CMCA** applies to any unauthorised use of computers and related materials, including any data contained therein, *whether the offender or computer or data is in Singapore or not*, for any offence which "causes, or creates a significant risk of, serious harm in Singapore."[297] "[S]erious harm in Singapore" involves:

- "a disruption of, or a serious diminution of public confidence in, the provision of any essential service";
- "a disruption of, or a serious diminution of public confidence in, the performance of any duty or function of, or the exercise of any power by" the Singapore government or any Singapore governmental agency; or
- "damage to the national security, defence or foreign relations of Singapore."[298]

An example would be giving the public access to confidential documents belonging to a Singapore governmental ministry.[299]

The **Cybersecurity Act** also empowers the minister to "authorise or direct any person or organisation" to "take such measures or comply with such requirements as may be necessary to prevent, detect or counter any threat to a computer or computer service" for the "for the purposes of preventing, detecting or countering any serious and imminent threat to (a) the provision of any essential service; or (b) the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore".[300] This may include the powers to access computers granted under the Criminal Procedure Code, including those discussed above.[301]

---

[294] PDPA s 21(3)(*e*).
[295] PDPA Second Schedule s 1(*d*), Third Schedule s 1(*d*), Fourth Schedule s 1(*e*).
[296] PDPA s 2(1).
[297] CMCA s 11.
[298] CMCA s 11(4).
[299] CMCA s 11.
[300] Cybersecurity Act s 23(1). Section 23 of the Cybersecurity Act essentially re-enacts, with slight modifications, section 15A of the CMCA.
[301] Cybersecurity Act s 23(2).

The Cybersecurity Act also authorises (among other things) the taking of measures to prevent, manage and respond to cybersecurity threats.[302] This has two general components – ensuring the protection of CIIs,[303] and preventing and investigating cybersecurity incidents.[304] See also Response 20-21.

It is also notable that section 58 of the Telecommunications Act seemingly provides a lower threshold for the minister to give directions to a telecommunications licensee, where it is "requisite or expedient to do so", "on the occurrence of any public emergency, in the public interest or in the interests of public security, national defence, or relations with the government of another country".[305]

VI. REMEDIES AND SANCTIONS

24. What remedies, if any, are available in your jurisdiction for the breach of the following data protection rules (please specify any administrative, civil and/or criminal remedies and the type of consequences, if any – e.g., fines, withdrawal of licenses, compensations, imprisonment of company's administrators or null evidence):

24.1. General personal data protection rules;

24.2. Rules regarding the protection of personal data in the context of services provided at a distance, by electronic means, at the individual request of a recipient of services;

24.3. Rules regarding the protection of personal data in the context of electronic communications for marketing purposes;

24.4. Rules regarding the electronic processing of personal data of employees;

24.5. Rules regarding the security of personal data processed by electronic means;

24.6. Rules regarding the processing of personal data in the electronic communications sector;

24.7. Rules applicable to the protection of personal data for the purpose of the investigation, detection and prosecution of crimes through electronic means;

24.8. Rules applicable to the electronic processing of personal data for security and national defence purposes.

25. In the event there is a supervisory body specific for any of the areas specified in the previous question, please indicate the maximum financial penalty or sanction that this supervisory body can issue and what is the maximum financial penalty or sanction that has been issued to date (please clarify if it is possible to appeal to courts).

Response 24-25

PDPA

Enforcement under the PDPA is complaints-based rather than audit-based.[306] However, the

[302] Cybersecurity Act (long title).
[303] Cybersecurity Act ss 7-10.
[304] Cybersecurity Act ss 19-23.
[305] Telecommunications Act s 58. See also Eugene KB Tan, "Security and privacy must not be traded off against each other". https://www.todayonline.com/commentary/security-and-privacy-must-not-be-traded-against-each-other. (Accessed 18 June 2018).
[306] Chesterman (para 1.96); PDPA s 50(1).

Commission may also conduct an investigation under the PDPA on its own motion.[307]

Remedies. The Commission may refer a complaint for mediation or direct the parties to resolve the complaint "in the way directed by the Commission."[308] Additionally, in response to a complaint regarding an organisation's non-compliance with the Access or Correction Obligations, the Commission may: confirm a refusal to provide access or direct the organisation to provide such access; confirm, reduce, or disallow a fee imposed in connection with such request, or require a refund of such fee; or confirm a refusal to correct data, or direct the organisation to correct such data.[309]

The Commission may also give a non-PDPA compliant organisation such directions as it sees fit, including to: stop collecting, using or disclosing personal data; destroy personal data collected in contravention of the PDPA; comply with the Commission's directions concerning the Access or Correction Obligations; and pay a penalty not exceeding SGD1 million (save for breaches which are offences under the PDPA).[310] The Commission may register its directions at a District Court for enforcement purposes.[311]

To date, the maximum penalty issued under the PDPA has been SGD50,000.[312] In practice, the Commission has also issued warnings in cases which it did not deem severe breaches of the PDPA.[313]

Offences. It is an offence to request for access to, or to change personal data about another individual without the authority of such individual, conviction under which may result in a fine not exceeding SGD5,000 and/or imprisonment for a term not exceeding 12 months.[314]

An organisation or person commits an offence if (a) with intent to evade a request under the Access or Correction Obligations, it/he/she disposes of, alters, falsifies, conceals or destroys (or directs another person to do any of the above) a record containing (i) personal data or (ii) information about the collection, use or disclosure of personal data; (b) obstructs or hinders the Commission in the performance of any function or duty, or the exercise of any power, under the PDPA; or (c) makes a statement or furnishes any information or document, to the Commission which it/he/she knows (or ought reasonably to know) to be false or misleading.[315] Conviction under (a) may result in, for an individual, a fine not exceeding SGD5,000 and otherwise a fine not exceeding SGD50,000.[316] Conviction under (b) or (c) may result in, for an individual, a fine not exceeding SGD10,000 and/or imprisonment for a term not exceeding 12 months, and otherwise a fine not exceeding SGD100,000.[317]

---

[307] PDPA s 50(1).
[308] PDPA s 27.
[309] PDPA s 28.
[310] PDPA s 29.
[311] PDPA s 30.
[312] *K Box Entertainment Group Pte. Ltd*. [2016] SGPDPC 1.
[313] See, eg, *Singapore Computer Society*, [2016] SGPDPC 09; *Jump Rope (Singapore)* [2016] SGPDPC 21. See also Response 13.
[314] PDPA s 51(1)-(2).
[315] PDPA s 51(3).
[316] PDPA s 51(4).
[317] PDPA s 51(5).

Regarding the DNCR provisions, each of the following is an offence which may result in a fine not exceeding SGD10,000:

- Sending a marketing message to a Singapore telephone number listed in a DNCR;[318]
- In sending a marketing message, failing to include certain contact and other information regarding the sending individual or organisation;[319]
- Making a marketing voice call that conceals the identity of the sender;[320]
- A telecommunications service provider's failure to report to the Commission all terminated Singapore telephone numbers.[321]

Finally, any person guilty of an offence under the PDPA "for which no penalty is expressly provided" shall be liable on conviction to a fine not exceeding SGD10,000 and/or imprisonment for a term not exceeding three years.[322] If it is a "continuing offence", there shall be "a further fine" not exceeding SGD1,000 for every day or part thereof during which the offence continues after conviction.[323]

Where an offence committed by a body corporate has been committed with the consent or connivance, or is attributable to the neglect of, an officer of such body, both the officer and the body shall be guilty of the offence.[324] Employers are also liable for an employee's acts done in the course of his/her employment, whether or not such act was done with the employer's knowledge or approval.[325] However, it is a defence for an employer to prove that he "took such steps as were practicable to prevent the employee" from doing such act.[326]

The courts have jurisdiction over offences under the PDPA.[327] However, the Commission may compound certain offences thereunder.[328]

Appeals. An organisation or individual may apply for reconsideration of the Commission's decision[329] or appeal such decision to the Data Protection Appeal Panel ("DPAP").[330] An appeal against the DPAP's decision may be made regarding a point of law or the amount of a financial penalty imposed to the Singapore High Court.[331] Further appeal to the Court of Appeal may be made, in the same manner as for High Court decisions made "in the exercise of its original civil jurisdiction."[332]

---

[318] PDPA s 43(2).
[319] PDPA s 44(2).
[320] PDPA s 45(2).
[321] PDPA s 42(2).
[322] PDPA s 56.
[323] PDPA s 56.
[324] PDPA s 52(1)-(2). This also applies to partnerships and unincorporated associations. PDPA s 52(3)-(4).
[325] PDPA s 53(1).
[326] PDPA s 53(2).
[327] PDPA s 54.
[328] PDPA s 55; Personal Data Protection (Composition of Offences) Regulations 2013 (S 759 of 2013). Available via Singapore Statutes Online. https://sso.agc.gov.sg.
[329] PDPA s 31(1).
[330] PDPA s 33 read with 34(1)-(2). If an application for reconsideration is made, an appeal on the same matter shall be deemed to be withdrawn: PDPA s 34(2).
[331] PDPA s 35(1).
[332] PDPA s 35(4).

Private actions. There is a right of private civil action by any person who suffers loss or damage "directly as a result of" a PDPA breach by an organisation.[333] A claimant may obtain damages, injunction or declaration, or such other relief as the court sees fit.[334] However, if the Commission has made a decision in respect of such breach, no private action may be brought until all appeals regarding such breach are exhausted.[335]

Criminal Procedure Code

It is an offence to breach the new computer-related powers of investigation under the recent amendments to the Criminal Procedure Code (by obstructing an investigation or failure to comply with an order).[336] The offender may receive a fine not exceeding SGD5,000 and/or imprisonment for a term not exceeding 6 months.[337] Where the offender is a body corporate, it may receive a fine not exceeding SGD10,000.[338]

CMCA

Under the CMCA, obtaining, retaining, supplying, transmitting or making available "personal information" obtained in violation of certain CMCA offences[339] may result, for first time offenders, in a fine not exceeding SGD10,000 and/or imprisonment for a term not exceeding three years; and on subsequent convictions, to a fine not exceeding SGD20,000 and/or imprisonment for a term not exceeding five years.[340]

"Enhanced punishment" is also available for certain CMCA offences[341] involving "protected computers," ie where the offender knew (or ought reasonably to have known) that the computer or program or data in question was used in directly connection with or was necessary for "the security, defence or international relations of Singapore"; "the existence or identity of a confidential source of information relating to the enforcement of a criminal law"; "the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure"; or "the protection of public safety including systems related to essential emergency services."[342] Conviction thereunder may result in a fine not exceeding SGD100,000 and/or to imprisonment not exceeding 20 years.[343] The courts have jurisdiction over all CMCA offences;[344] however, the certain offences thereunder may be compounded.[345]

Private action. There is a right of private civil action under the CMCA. A court which has convicted a person under the CMCA may also order him/her to make compensation to a person

[333] PDPA s 32(1).
[334] PDPA s 32(3).
[335] PDPA s 32(2).
[336] CJRB c 9(3).
[337] CJRB c 9(3).
[338] CJRB c 9(3).
[339] CMCA ss 3-6.
[340] CMCA s 8A.
[341] CMCA ss 3, 5-7.
[342] CMCA s 9(1)-(2).
[343] CMCA s 9(1).
[344] CMCA s 12.
[345] CMCA s 12A.

"for any damage caused to his computer, program or data."[346] Such claim shall also "not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order."[347]

Cybersecurity Act
Regarding measures taken and/or requirements to prevent, detect or counter threats to Singapore's national security, essential services, defences or foreign relations, obstruction of such measures or failure to comply with such requirements is an offence, conviction of which may result in a fine not exceeding SGD50,000 and/or imprisonment not exceeding 10 years.[348] Additionally, a person with information pursuant to the above measures and/or requirements who uses or discloses such information has committed an offence, conviction under which may result in a fine not exceeding SGD10,000 and/or imprisonment for a term not exceeding 12 months.[349]

PS(G)A
Public servants who share data (including personal data) without authorisation, or who make use of data to benefit themselves, can be fined up to $5,000 and/or jailed for up to two years.[350] Public servants who re-identify (or cause re-identification of) anonymised data without authorisation are also liable for the same punishment.[351]

VII. PRIVATE INTERNATIONAL LAW RULES

26. How is the territorial scope of application of data protection rules, including rules on electronic data processing, defined in your jurisdiction?

The PDPA applies to all organisations carrying out activities involving personal data in Singapore.[352] Any organisation that collects personal data overseas and brings it into Singapore is also subject to the PDPA from the time it seeks to collect the personal data (if such collection occurs in Singapore) or brings such data into Singapore.[353] See Responses 13 (data intermediaries).

Regarding personal data implicated in computer-related crimes, under the CMCA Singapore claims extra-territorial jurisdiction over any person or any data which causes or creates a significant risk of serious harm in Singapore.[354] (See Response 22-23 for the definition of "serious harm".) Under the Criminal Procedure Code, investigators can also inspect and search

[346] CMCA s 13(1).
[347] CMCA s 13(2).
[348] Cybersecurity Act s 23(4)-(5).
[349] CMCA s 15A(8)-(9).
[350] PS(G)A s 7(1), (3).
[351] PS(G)A s 8.
[352] Advisory Guidelines on Key Concepts para 11.1.
[353] Advisory Guidelines on Key Concepts para 11.2. See also Lim, HYF (2014) Data Protection in the Employment Setting (para 5.15: "[t]he reach of the PDPA [was] explicitly extended to those organisations that may not have any presence in Singapore, or which may not even be recognised under the law of Singapore"). In: Chesterman, S (ed) Data protection law in Singapore: privacy and sovereignty in an interconnected world. Academy Publishing, Singapore.
[354] CMCA s 11.

any data stored on or available to a computer implicated in the investigation, regardless of whether the computer is inside or outside Singapore (thus this could include web-based email accounts and web storage accounts).[355]

27. Is electronic data processing by entities seated outside your jurisdiction comprised in the scope of application of local rules?

Response 27

Under the PDPA, yes, so long as the personal data is located in Singapore. Indeed, the definition of "organisation" includes companies formed under non-Singapore laws and/or resident outside Singapore.[356]

Regarding personal data implicated in computer-related crimes, under the CMCA Singapore claims extra-territorial jurisdiction over any person or any data which causes or creates a significant risk of serious harm in Singapore.[357] (See Response 22-23 for the definition of "serious harm".) Under the Criminal Procedure Code, investigators can also inspect and search any data stored on or available to a computer implicated in the investigation, regardless of whether the computer is inside or outside Singapore (thus this could include web-based email accounts and web storage accounts).[358]

For the Cybersecurity Act, a computer/computer system has to be located wholly or partly in Singapore to be considered a CII.[359] The PS(G)A does not discuss this issue; however it covers generally data "under the control" of an agency.[360]

28. Is the transfer of personal data to a foreign jurisdiction freely allowed or subject to specific conditions? If yes, what are they?

Response 28

No personal data shall be transferred outside Singapore unless the recipient of that data is bound by legally enforceable obligations to provide the transferred data a standard of protection that is at least comparable to the protection afforded under the PDPA.[361] "Legally enforceable obligations" includes obligations imposed on the recipient under: any law; the use of contractual arrangements; and/or binding corporate rules (for intra-corporate transfers only).[362]

The above requirement is also satisfied if, among others: the individual concerned consents to the data transfer; the transfer is necessary for the performance of a contract between the individual and the organisation; the transfer is necessary for a use or disclosure in certain situations where consent is not required under the PDPA; the data is merely in transit through

[355] CJRB c 9(*a*)(1).
[356] PDPA s 2(1).
[357] CMCA s 11.
[358] CJRB c 9(*a*)(1).
[359] Cybersecurity Act s 7(1)(*b*).
[360] PS(G)A s 6(1).
[361] PDPA s 26(1); PDPR s 9(1).
[362] PDPR s 10; Advisory Guidelines on Key Concepts para 19.2.

Singapore; or the data is publicly available in Singapore.[363] Additionally, exemptions may be granted.[364]

29. What law applies to liability for damages caused by the unlawful processing of personal data in your jurisdiction?

Response 29
Singapore law will apply. See Response 24-25.

[363] PDPR s 9(3).
[364] PDPA s 26(2).