Assessment of the Singapore Personal Data Protection Act 2012 (2020 Revised Edition) ("PDPA") and the Cross Border Privacy Rules ("CBPR") for an Adequacy Recognition Decision by the Dubai International Financial Centre Authority ("DIFC" or "DIFCA")

Office of the Commissioner of Data Protection

DIFC

Table of Contents

DIFC

Introduction

Articles 26 and 27 of the Data Protection Law, DIFC Law No. 5 of 2020 and Section 5 of the DIFC Data Protection Regulations 2020 (the "DIFC DP Law 2020"[1]) address transfers of Personal Data to Third Countries or International Organizations. Article 26(2) specifically states:

> *For the purposes of Article 26(1), the Commissioner may determine from time to time that a Third Country, a territory or one (1) or more specified sectors within a Third Country, or an International Organisation ensures an adequate level of data protection*.

Such adequacy recognition is based on an assessment of key data protection concepts and obligations found in a jurisdiction's data protection laws to ensure equivalence with the local data protection law[2].

As such, the DIFC Office of the Commissioner of Data Protection (the "DIFC Commissioner") assesses Singapore's laws and regulations according to the following criteria:

1. Basic data protection concepts and definitions
2. Grounds for lawful and fair processing for legitimate purposes
3. Existence of Data Protection Principles
    a. purpose limitation
    b. data quality and proportionality
    c. data retention
    d. security and confidentiality
    e. transparency
4. Data Subjects' Rights
5. International / Onward Data Transfer Restrictions
6. Security of Processing and Breach Reporting
7. Accountability, Redress and Enforcement
8. Additional content principles for specific types of processing, such as:
    a. Special categories of data (aka sensitive personal data)
    b. Direct marketing
    c. Automated decision making and profiling
9. Existence of international commitments and conventions binding on Singapore or its membership of any multilateral or regional organisations.

[1] *All definitions and capitalized terms herein, including the definition of the DIFC Data Protection Commissioner, are as set out in DIFC DP Law 2020, Schedule 1, Article 3.*

[2] *Please see DIFC's Data Export and Sharing page for additional information.*

Summary of Singapore's Applicable Laws and Regulations

The Singapore data protection regime is built upon the Personal Data Protection Act 2012 (the "PDPA"). A draft Personal Data Protection (Amendment) Bill ("Amendment Bill") was passed in the Singapore Parliament in November 2020. The Amendments were adopted and enacted 1 February 2021.

The DIFC Commissioner's Offices has reviewed the PDPA and relevant portions of the Amendment Bill, against similar provisions in the DIFC DP Law 2020[3], and provides its findings below.

[3] *For any additional information about the DIFC DP Law 2020, including FAQs, Guidance, Assessment Tools, or other useful forms, please go to the DIFC Data Protection website.*

Observation 1: Basic data protection concepts and definitions

Concepts:

Definitions are found in Part 1, Article 2 of the PDPA. While they somewhat vary from the DIFC definitions, there are substantial similarities with the DIFC DP Law 2020 when interpreted accordingly. The PDPA applies to organizations and data intermediaries, akin to Controllers and Processors. Personal Data is defined quite similarly, and includes the data of living or dead individuals. Further interpretation is found in guidance. For example there is no sensitive Personal Data definition, and the PDPA is not applicable to business-related Personal Data or data collected for mixed purposes. Guidance does apply, however:

> *Non-binding guidance from the Singapore Personal Data Protection PDP Commission (the PDPC) indicates that sensitivity of data is a factor for consideration in implementing policies and procedures to ensure appropriate levels of security for Personal Data. For example, encryption is recommended for sensitive data stored in an electronic medium that has a higher risk of adversely affecting the individual should it be compromised. Where any Personal Data collected is particularly sensitive (e.g., regarding physical or mental health), as a matter of best practice, such data should only be used for limited purposes and the security measures afforded to such data should take into account the sensitivity of the data.*

The PDPA provides that the Data Protection Provisions do not impose any obligations on the following entities. These categories of Organisations are therefore excluded from the application of the Data Protection Provisions:

a. Any individual acting in a personal or domestic capacity;

b. Any employee acting in the course of his or her employment with an Organisation; and

c. Any public agency.

Organisations which are not within an excluded category are in any case required to comply with the PDPA when dealing with an Organisation that is within an excluded category.

The main Personal Data principles under the PDPA are substantially the same as in the DIFC, as follows:

- Consent Obligation
- Purpose Limitation
- Privacy Notices
- Access and Correction
- Accuracy
- Protection / Security
- Retention Limitation
- Transfer Limitation

- Data Breach Notification
- Accountability

Organizations must ensure that they provide clear, understandable privacy notices that set out data subjects' rights, and upon request, must ensure that every reasonable step is taken to provide access to Personal Data, to permit and resolve objections to processing, and to erase or rectify Personal Data that is inaccurate, incomplete, or processed in a manner that is incompatible with regard to the purpose for which it was collected.

Organizations must also establish and maintain systems and controls, including technical and organizational measures and appropriate policies that enable it to satisfy itself that it complies with the requirements set out in the PDPA.

Observation 2: Grounds for lawful and fair processing for legitimate purposes

Requirements for legitimate processing and processing of Sensitive Personal Data are generally included in Schedule 2 of the PDPA. There are clear and substantial similarities with the DIFC DP Law 2020 when interpreted accordingly, in line with Articles 9, 10, 11, 12, 13 and 22 of DIFC DP Law 2020.

https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=Sc2-XX-Sc2-#Sc2-XX-Sc2-

Organizations may only collect, use or disclose Personal Data in the following scenarios:

They obtain express consent from the individual prior to the collection, use, or disclosure of the Personal Data (and such consent must not be a condition of providing a product or service, beyond what is reasonable to provide such product or service; and must not be obtained through the provision of false or misleading information or through deceptive or misleading practices), and have also provided the relevant data protection notice (notifying purposes of collection, use and disclosure) to the individual before, or at the time when they are collecting, using or disclosing the Personal Data

There is deemed consent by the individual to the collection, use, or disclosure of the Personal Data in accordance with the relevant conditions of the PDPA.

Where the limited specific exclusions prescribed in the PDPA apply (if no consent or deemed consent is given).

Such exclusions include vital interests of individuals, matters affecting public, legitimate interests, business asset transactions, business improvement purposes and other additional bases.

The Amendment Bill expanded the concept of “deemed consent” to cover circumstances where: (i) the collection, use or disclosure of Personal Data is reasonably necessary to conclude or perform a contract or transaction; or (ii) where individuals have been notified of the purpose of the intended collection, use or disclosure of Personal Data, given a reasonable opportunity to opt-out, and have not opted out.

An individual may at any time withdraw any consent given, or deemed given under the PDPA, upon giving reasonable notice to the organization.

Observation 3: Existence of Data Protection Principles

Data protection principles, as found in Parts 2A, 2B and 2C of the DIFC DP Law, are found as well in the PDPA. These are set out below.

1. Consent

An Organisation may collect, use and/or disclose only the Personal Data of individuals who have consented to collection, use and/or disclosure. Individuals must also have the ability to withdraw consent upon reasonable notice of such withdrawal. At this point the Organisation must cease collecting, using and/or disclosing the Personal Data of these individuals. This obligation is similar to Articles 13 and 22 of the DP Law 2020.

2. Purpose Limitation

An Organisation may collect, use and/or disclose only the Personal Data of individuals for the purpose(s) for which consent has been given. Consent can never be mandatory for any purpose given by the Organisation to provide a particular product or service unless consent is required for a reasonable purpose of providing such service. This obligation is similar to Article 9(1)(c) of the DP Law 2020.

3. Privacy notices

An Organisation must inform individuals of the purpose(s) for which their Personal Data is being collected, used and/or disclosed. Privacy notices are required under Articles 29 and 30 of the DP Law 2020.

4. Access and Correction

An Organisation is obliged to provide information to individuals, upon request and as soon as reasonably possible, on:

- What Personal Data of theirs is in the Organisation's possession or under its control; and
- How such Personal Data has been used or disclosed within 1 year of the request.

Also, should an individual request that the organization rectify any error or omission in his or her Personal Data, the Organisation must accede to the request as soon as practicable.

These requirements are substantially similar to those found in Articles 9(1)(f) and Articles 32 to 40 of the DP Law 2020.

5. Accuracy

An Organisation must ensure that the Personal Data it collects accurate and complete. Please see Article 9(1)(g) of the DP Law 2020.

6. Protection / Security

An Organisation must implement security measures to protect the Personal Data in its possession or control, including the storage media or devices on which such data is stored in order to prevent unauthorised access, collection, use and/or disclosure of such data. This requirement is found in Article 9(1)(i) of the DP Law 2020.

7. Retention

An Organisation should retain the Personal Data only for as long as is necessary for business or legal purposes. This requirement is found in Article 9(1)(h) of the DP Law 2020.

8. Cross Border Transfers

If an Organisation is transferring Personal Data overseas, such as storing the data in the cloud, it must ensure that the country to which the data is being transferred offers a comparable level of data protection as is provided by the PDPA. This requirement is found in Articles 26 and 27 of the DP Law 2020.

9. Data Breach Notifications

If an Organisation has suffered a data breach that has caused (or is likely to cause) significant harm to affected individuals, or that has affected at least 500 individuals, then it generally must inform the PDPC and affected individuals of the breach. Similar requirements are found in Articles 41 and 42 of the DP Law 2020.

10. Accountability

An Organisation should be transparent and accountable for its data protection practices, policies and complaints processes upon request. This includes maintaining privacy policies, appointing someone responsible for data protection operations, such as a data protection officer (“DPO”), and must also provide a way of contacting the DPO. Similar requirements are found in Articles 14 to 22 of the DP Law 2020.

The above principles (obligations) are referenced in the following sections of the PDPA and in the associated guidance (updated in 2021):

Consent requirements are found in Part IV, Division 1
https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P1IV-#P1IV-P21-

Purpose limitation is found in Part IV, Division 2

https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P1IV-#pr18-

Data retention is found in Part VI, Article 25

https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P1VI-#pr25-

Accuracy is covered by Part VI, Article 23

https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P1VI-#pr23-

Access and Correction of Personal Data are found in Part V, Article 21, 22 and 22A
https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P1IV-#P1IV-P21-

Security / Protection of Personal Data is covered in Part VI, Article 24

https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P1VI-#pr24-XX-pr24-

Transfer of Personal Data is covered in Part VI, Article 26

https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P1VI-#pr26-

Notification of breaches of Personal Data is covered in Part VIA, Articles 26A to 26E

https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P1VIA-#P1VIA-

Accountability for processing of Personal Data is covered in Part III, Articles 11 and 12

https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P1III-#P1III-

Observation 4: Data Subjects Rights (DSR)

DIFC DP Law 2020 provides for DSR in Part 6. It contains substantially similar rights as are found in the PDPA.

From the guidance, Section 15, provided by the PDPC, Sections 21, 22 and 22A of the PDPA set out the rights of individuals to request for access to their Personal Data and for correction of their Personal Data that is in the possession or under the control of an Organisation, and the corresponding obligations of the Organisation to provide access to, and correction of, the individual's Personal Data. These obligations are collectively referred to as the Access and Correction Obligations as they operate together to provide individuals with the ability to verify their Personal Data held by an organization.

The Access and Correction Obligations relate to Personal Data in an Organisation's possession as well as Personal Data that is under its control (which may not be in its possession). For example, if an Organisation has transferred Personal Data to a data intermediary that is processing the Personal Data under the control of the Organisation, the Organisation's response to an access or correction request must take into account the Personal Data which is in the possession of the data intermediary. The PDPA does not directly impose the Access and Correction Obligations on a data intermediary in relation to Personal Data that it is processing only on behalf of and for the purposes of another Organisation pursuant to a contract which is evidenced or made in writing. A data intermediary may (but is not obligated under the PDPA to) forward the individual's access or correction request to the Organisation that controls the Personal Data. The PDPC understands that, in some cases, an Organisation may wish to enter into a contract with its data intermediary for the data intermediary to assist with responding to access or correction requests on its behalf. In this connection, the PDPC would remind Organisations that engage the data intermediary, that they remain responsible for ensuring compliance with the Access and Correction Obligations under the PDPA.

Also, it is worth noting that if the Personal Data requested by the individual can be retrieved by the individual himself (e.g. resides in online portals in which access has been granted by the Organisation), the Organisation may inform the individual how he may retrieve the data requested.

Regarding the obligation to specify how the Personal Data has been or may have been used or disclosed within the past year, Organisations may provide information on the purposes rather than the specific activities for which the Personal Data had been or may have been used or disclosed. For example, an Organisation may have disclosed Personal Data to external auditors on multiple occasions in the year before the access request. In responding to an access request, the Organisation may state that the Personal Data was disclosed for audit purposes rather than describing all the instances when the Personal Data was disclosed.

Organisations are not required to accede to a request if an exception, set out in Fifth Schedule of the PDPA, from the access requirement applies.
The exceptions specified in the Fifth Schedule include the following matters:

a. opinion data kept solely for an evaluative purpose;

b. any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results;

c. the Personal Data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;

d. Personal Data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre;

e. a document related to a prosecution if all proceedings related to the prosecution have not yet been completed;

f. Personal Data which is subject to legal privilege;

g. Personal Data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the Organisation;

h. Personal Data collected, used or disclosed without consent for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed;

i. Personal Data collected by an arbitrator or mediator in the conduct or an arbitration or mediation for which he or she was appointed to act –

   i. under a collective agreement under the Industrial Relations Act 1960;
   ii. by agreement between the parties to the arbitration or mediation;
   iii. under any written law; or
   iv. by a court, arbitral institution or mediation centre; or

j. any request —

   i. that would unreasonably interfere with the operations of the Organisation because of the repetitious or systematic nature of the requests (i.e. considering the number and frequency of requests received);
   ii. if the burden or expense of providing access would be unreasonable to the Organisation or disproportionate to the individual's interests;
   iii. for information that does not exist or cannot be found;
   iv. for information that is trivial; or
   v. that is otherwise frivolous or vexatious.

Additionally, an Organisation shall not inform any individual or Organisation that it has disclosed Personal Data to a prescribed law enforcement agency if the disclosure is necessary for any investigation or proceedings and the Personal Data is disclosed to an authorised officer of the agency. In this regard, an Organisation may refuse to confirm or deny the existence of Personal Data, or the use of Personal Data without consent for any investigation or proceedings, if the investigation or proceedings and related appeals have not been completed.

Organisations have 30 days to respond, and may request an additional 30 days. Organisations may also provide a quote for fees to cover incremental costs of the search only.

Observation 5: International Data Transfers

Like Articles 26 and 27 of the DIFC DP Law 2020, an Organisation subject to the PDPA may transfer Personal Data overseas if it has taken appropriate steps to ensure that the overseas recipient is bound by legally enforceable obligations or specified certifications to provide the transferred Personal Data a standard of protection that is comparable to that under the PDPA.

Legally enforceable obligations may be imposed in two ways. First, it may be imposed on the recipient Organisation under:

a. any law;

b. any contract that imposes a standard of protection that is comparable to that under the PDPA, and which specifies the countries and territories to which the Personal Data may be transferred under the contract;

c. any binding corporate rules that48 require every recipient of the transferred Personal Data to provide a standard of protection for the transferred Personal Data that is comparable to that of the PDPA, and which specify

   i. the recipients of the transferred Personal Data to which the binding corporate rules apply;
   ii. the countries and territories to which the Personal Data may be transferred under the binding corporate rules; and
   iii. the rights and obligations provided by the binding corporate rules; or

d. any other legally binding instrument.

Second, if the recipient Organisation holds a "specified certification" that is granted or recognised under the law of that country or territory to which the Personal Data is transferred, the recipient Organisation is taken to be bound by such legally enforceable obligations. Under the Personal Data Protection Regulations 2021, "specified certification" refers to certifications under the Asia Pacific Economic Cooperation Cross Border Privacy Rules ("APEC CBPR") System, and the Asia Pacific Economic Cooperation Privacy Recognition for Processors ("APEC PRP") System. The recipient is taken to satisfy the requirements under the Transfer Limitation Obligation if:

a. it is receiving the Personal Data as an Organisation and it holds a valid APEC CBPR certification; or

b. it is receiving the Personal Data as a data intermediary and it holds either a valid APEC PRP or CBPR certification, or both.

In setting out contractual clauses that require the recipient to comply with a standard of protection in relation to the Personal Data transferred to him that is at least comparable to the protection under the PDPA, a transferring Organisation should minimally set out protections with regard to the data protection obligations. The position under the PDPA is that certain Data Protection Provisions are not imposed on a data intermediary in respect of its processing of Personal Data on behalf of and for the purposes of another Organisation pursuant to a contract that is evidenced or made in writing. However, it is expected that Organisations engaging such data intermediaries would generally have imposed obligations that ensure adequate protection in the relevant areas in their processing contract. The PDPC also recognises and encourages the use of the ASEAN Model Contract Clauses ("MCCs"), which are contractual terms setting out baseline responsibilities, required

Personal Data protection measures, and related obligations of the parties that protects the data of individuals, to fulfil the Transfer Limitation Obligation. DIFC likewise has issued standard contractual clauses as documented in the Data Protection Regulations 2020, Regulation 5[4]. The DIFC SCCs align with other similar clauses and transfer mechanisms, including the Cross Border Privacy Rules (CBPR) – please see Observation 9 below.

Data in transit is treated as it is in the DIFC, EU, UK, etc.

[4] *Please see the Model Clauses section of the DIFC Data Export & Sharing website*

Observation 6: Security of Processing and Breach Reporting

Security

Organizations must protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification, disposal, the loss of any storage medium or device on which personal data is stored, or similar risks. Data intermediaries are also directly liable and subject to the same security obligation. The Act does not specify security measures to adopt and implement, however the PDPC has issued best practice guidance which provides specific examples, including with respect to cloud computing and IT outsourcing.

Breach Reporting

An organisation must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a "notifiable breach" if there is reason to believe that a data breach affecting personal data in its possession or under its control has occurred. A data breach constitutes a "notifiable breach" if:

- it results in, or is likely to result in, significant harm to the affected individuals; or
- it is of a significant scale (i.e. one that affects 500 or more individuals).

An organisation must notify the PDPC as soon as practicable and in any case no later than three calendar days after the aforementioned assessment, and in the second case, must also notify each affected individual in any reasonable manner.

The Personal Data Protection (Notification of Data Breaches) Regulations 2021 sets out the list of information to be included in notifications to the PDPC and affected individuals.

Intermediaries must, in relation to personal data that it is processing on behalf of an organization, must notify other organisations, i.e. a data controller, likewise without undue delay from the time it has reason to believe a breach occurred. The organisation must then assess whether it is a notifiable data breach.

Observation 7: Accountability, Redress and Enforcement

Data Protection Officers (DPO) must be appointed under the PDPA. The DIFC DP Law 2020, Articles 16 to 19, do not contain mandatory DPO appointment provisions, but it is mandatory for DIFC Bodies (i.e., government authorities in the DIFC), those undertaking high risk processing (HRP), and those directed to do so by the Commissioner of Data Protection[5].

Section 12 of the PDPA sets out four additional key requirements which form part of the Accountability Obligation. Firstly, an Organisation is required to develop and implement data protection policies and practices to meet its obligations under the PDPA. Policies can be internal or external facing; and practices can include establishing governance structures and designing processes to operationalise policies. Organisations should develop policies and practices by taking into account matters such as the types and amount of Personal Data it collects, and the purposes for such collection. This also entails ensuring that policies and practices are easily accessible to the intended reader. Furthermore, the Organisation should put in place monitoring mechanisms and process controls to ensure the effective implementation of these policies and practices.

Secondly, an Organisation must develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA. This is to ensure that the Organisation can effectively address individuals' complaints and concerns with its data protection policies and practices and aid in its overall compliance efforts.

Thirdly, an Organisation is required to provide staff training and communicate to its staff information about its policies and practices. Such communication efforts could be incorporated in Organisations' training and awareness programmes and should include any additional information which may be necessary for the Organisation's staff to effectively implement its data protection policies and practices. An effective training and awareness programme builds a staff culture that is sensitive and alert to data protection issues and concerns.

Finally, an Organisation is required to make information available on request concerning its data protection policies and practices and its complaint process. This is to ensure that individuals are able to find the necessary information and, if necessary, have the means of raising any concerns or complaints to the Organisation directly.

In general, an Organisation's Personal Data protection policies and practices set the tone for the Organisation's treatment of Personal Data, and provide clarity on the direction and manner in which an Organisation manages Personal Data protection risks. These should be developed to address and suit specific business or Organisational needs. Please refer to the PDPC's website for resources on demonstrating Organisational accountability.

The Data Protection Provisions also provide for specific circumstances where Organisations have to be answerable to individuals and the PDPC, and be prepared to address these parties in an accountable manner. For example:

a. individuals may request for access to their Personal Data in the possession or under the control of an Organisation, which enables them to find out which of their Personal Data may be held by an Organisation and how it has been used;

[5] *Please see the Commissioner's guidance on what constitutes HRP, as well as HRP and DPO appointment assessment tools*

b. Organisations have to notify the PDPC and/or affected individuals when a data breach is likely to result in significant harm or is of a significant scale;

c. Organisations have to conduct risk assessments to identify and mitigate adverse effects for certain uses of Personal Data such as for legitimate interests;

d. individuals may submit a complaint to the PDPC and the PDPC may review or investigate an Organisation's conduct and compliance with the PDPA;

e. the PDPC may, if satisfied that an Organisation has contravened the Data Protection Provisions, give directions to the Organisation to ensure compliance including (amongst others) imposing a financial penalty of up to $1 million (or in due course, up to $1 million or 10% of the Organisation's annual turnover in Singapore, whichever is higher); and

f. individuals who suffer loss or damage directly as a result of a contravention of Parts 4, 5, 6 or 6A of the PDPA by an Organisation may commence civil proceedings against the organization.

Although not expressly provided for in the PDPA, Organisations may wish to consider demonstrating Organisational accountability through measures such as conducting Data Protection Impact Assessments ("DPIA") in appropriate circumstances, adopting a Data Protection by Design ("DPbD") approach, or implementing a Data Protection Management Programme ("DPMP"), to ensure that their handling of Personal Data is in compliance with the PDPA. Although failing to undertake such measures is not itself a breach of the PDPA, it could, in certain circumstances, result in the Organisation failing to meet other obligations under the PDPA. For example, an Organisation that does not conduct a DPIA may not fully recognise risks to the Personal Data it is handling within its IT infrastructure. This, in turn, may result in the Organisation failing to implement reasonable security measures to protect such data and hence committing a breach of section 24 of the PDPA.

Redress[6]:

An individual may have a right to redress where he or she can prove loss or damage arising out of the contravention, which may prove difficult but not impossible, and would require engaging in civil proceedings. Otherwise, where privacy laws from a foreign jurisdiction have extraterritorial effect, the law may have application in Singapore. Complaint mechanisms are also available and often more effective.

PDPC Advisory Guidelines provide further detail: Advisory-Guidelines-on-Enforcement-of-DP-Provisions-1-Feb-2021.pdf (pdpc.gov.sg)

36. Rights of private action

36.1 Section 48O(1) of the PDPA provides that any person who suffers loss or damage directly as a result of a contravention by an organisation of any provisions in Part 4, 5, 6, 6A or 6B or by a person of any provision of Division 3 of Part 9 or 9A may commence civil proceedings in the

[6] *Singapore High Court Interprets The Scope Of An Individual's Right To Bring A Private Action To Enforce A Contravention Of The Personal Data Protection Act 2012 - Privacy - Singapore (mondaq.com)*

courts against the organisation. Under section 48O(3) of the PDPA, a court hearing an action under section 49O(1) of the PDPA may grant any or all of the following:

36.1.1 an injunction or a declaration;
36.1.2 damages;
36.1.3 such other relief as the court thinks fit.

36.2 Where the Commission has made a decision under the PDPA in respect of a contravention, no action may be brought under section 48O(1) of the PDPA in respect of that contravention until the decision has become final as a result of there being no further right of appeal.

36.3 As the Commission is not empowered to award damages or other relief noted above to a complainant, persons who suffer loss or damage as a result of a contravention of the PDPA may commence civil proceedings directly. In general, such persons may wish to obtain legal advice in relation to their claim and possible civil proceedings.

36.4 Under the Rules of Court, where a party (referred to as the plaintiff) commences civil proceedings for relief under section 48O(1) of the PDPA, he is required to serve a copy of the writ or originating summons to the Commission not later than 7 days after service of the writ or originating summons on the defendant. In addition, any person who is granted a judgment or order by a court pursuant to section 48O of the PDPA is required to transmit a copy of the judgment or order to the Commission within 3 days after the date of the judgment or order.

Observation 8: Additional content principles for specific types of processing (including sharing for the purposes of law enforcement)

Electronic marketing activities are regulated under the Spam Control Act (Cap 311A) ("SCA"), to the extent that such activities involve the sending of unsolicited commercial communications in bulk by electronic mail or by SMS or MMS to a mobile telephone number.

The Amendment Bill extended the DNC provisions to include a prohibition on sending messages to telephone numbers generated or obtained through dictionary attacks (generating telephone numbers by combining numbers into numerous permutations) or address-harvesting software. The Amendment Bill also amends the SCA to prohibit sending unsolicited electronic messages to instant messaging accounts.

Also, DNC Regulations 2013 apply

https://sso.agc.gov.sg/SL/PDPA2012-S709-2013?DocDate=20210129

Please also see Observation 4 above.

Observation 9: Existence of international commitments and conventions binding on Singapore and its membership in the CBPR System

Singapore is one of nine APEC economies to have joined the Cross Border Privacy Rules (CBPR) to date — the others include United States, Mexico, Canada, Japan, South Korea, Chinese Taipei, Australia and the Philippines. Singapore also participates in the Privacy Recognition for Processors (PRP) framework.

As part of this adequacy assessment, the Commissioner's Office also recognizes the CBPR and PRP for onward transfers to entities operating within this framework, and applying such rules as set out in the related informational website:

https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system

Further information about the PRP is found here:

https://www.pdpc.gov.sg/help-and-resources/2021/10/apec-cross-border-privacy-rules-and-privacy-recognition-for-processors-systems#:~:text=APEC%20Privacy%20Recognition%20For%20Processors,of%20a%20controller's%20privacy%20requirements.

Conclusion

All elements that substantiate DIFCA recognition of adequacy are generally present. General principles, objectives and functions, accountability, enforcement and supervision, data subjects' rights, the establishment of an independent Commissioner, and other supporting requirements and obligations are essentially the same as the Data Protection Law, DIFC Law No. 5 of 2020.

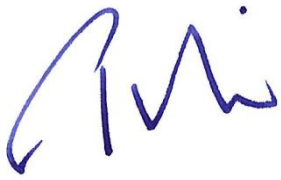
In addition to the relevant compatible elements of the PDPA and the DIFC DP Law 2020 set out above, the PDPC implemented the PDPA and its 2021 updates, and is committed to continuous improvement of inspections, investigations, and supervisory activities. Related to this, Singapore and DIFC Commissioner's Offices share a common objective of reviewing regulatory effectiveness through continuous improvement processes and updates to supervisory activities.

The DIFC Commissioner therefore grants provisional adequacy recognition to Singapore and the CBPR as ensuring adequate data protection in accordance with Article 26 of the DP Law 2020.

It is recommended that this decision is reviewed and where appropriate reconfirmed on an annual basis. The Commissioner has the right to repeal, amend or suspend this adequacy decision by notification to Singapore PDPC at any time.

This decision shall be reviewed annually.

Dated: February 4, 2022



_____

Jacques Visser
DIFC Commissioner of Data Protection

Appendix 1: Enforcement Action

Data Protection Enforcement

Please see the following guidance:

https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-on-Enforcement-of-DP-Provisions-1-Feb-2021.pdf?la=en

A list of enforcement decisions may be found here:

https://www.pdpc.gov.sg/Enforcement-Decisions

Appendix 2: Understanding and acknowledgement of Article 28 of the DIFC DP Law 2020

Article 28 of the DIFC DP Law 2020 states the following:

Data sharing

(1) Subject to any other obligations under this Law and, in particular, a Controller's or Processor's obligations under Part 2 regarding accountability, transparency and compliance with general data protection principles or Part 4 regarding transfers out of the DIFC, where a Controller or Processor receives a request from any public authority over the person or any part of its Group ("a Requesting Authority") for the disclosure and transfer of any Personal Data, it should:

(a) exercise reasonable caution and diligence to determine the validity and proportionality of the request, including to ensure that any disclosure of Personal Data in such circumstances is made solely for the purpose of meeting the objectives identified in the request from the Requesting Authority;

(b) assess the impact of the proposed transfer in light of the potential risks to the rights of any affected Data Subject and, where appropriate, implement measures to minimise such risks, including by redacting or minimising the Personal Data transferred to the extent possible or utilising appropriate technical or other measures to safeguard the transfer; and

(c) where reasonably practicable, obtain appropriate written and binding assurances from the Requesting Authority that it will respect the rights of Data Subjects and comply with the general data protection principles set out in Part 2 in relation to the Processing of Personal Data by the Requesting Authority.

(2) A Controller or, as applicable, its Processor(s) or any Sub-processor(s), having provided (where possible under Applicable Law) reasonable notice to the Controller, may disclose or transfer Personal Data to the Requesting Authority where it has taken reasonable steps to satisfy itself that:

(a) a request by a Requesting Authority referred to in Article 28(1) is valid and proportionate; and

(b) the Requesting Authority will respect the rights of Data Subjects in the Processing of any Personal Data transferred to it by the Controller pursuant to a request under Article 28(1).

(3) A Controller or Processor may consult with the Commissioner in relation to any matter under this Article 28.

The expectation of the DIFC Commissioner's Office is that these requirements will be considered, and where possible, applied, when relevant entities share Personal Data with government authorities in Singapore.