PUBLIC CONSULTATION PAPER NO. 03/2024:

THE RIGHT TO DATA PORTABILITY

PART 1: INTRODUCTION AND BACKGROUND

[A] Introduction

1.1 The Personal Data Protection (Amendment) Bill 2024 ("**Amendment Bill**"), which introduces amendments to the Personal Data Protection Act 2010 ("**PDPA**"), was passed without amendments by the House of Representatives on 16 July 2024, and by the Senate on 31 July 2024. The Amendment Bill is currently pending assent by the Yang di-Pertuan Agong.

1.2 Clause 9 of the Amendment Bill seeks to introduce a new right of a data subject to data portability subject to technical feasibility and compatibility of the data format by inserting a new Section 43A under Part II of the PDPA.

1.3 For ease of reference, the full text of Section 43A of the PDPA which provides for the new right to data portability states as follows:

> ***Rights to data portability***
>
> ***43A.*** *(1) Subject to subsection (2), a data subject may request the data controller to transmit his personal data to another data controller of his choice directly by giving a notice in writing by way of electronic means to the data controller.*
>
> *(2) The request for data portability referred to in subsection (1) is subject to technical feasibility and compatibility of the data format.*
>
> *(3) Upon receiving the request for data portability under subsection (1), the data controller shall complete the transmission of personal data within the period as may be prescribed.*

1.4 In essence, the "**right to data portability**" is the right of a data subject to request the transmission of personal data from a data controller to a receiving data controller. A "**data portability request**" must be made by the data subject in writing and submitted to the transmitting data controller electronically.

1.5 To supplement the new right to data portability that will be introduced by the new Section 43A of the PDPA, a proposed Personal Data Protection (Right to Data Portability) Regulations ("**Data Portability Regulations**") and Data Portability Guidelines ("**Data Portability Guideline**") are being developed by the Personal Data Protection Commissioner ("**Commissioner**"). The Data Portability Regulations and the Data Portability Guideline will provide additional guidance on interpretation and implementation of the data portability right and supplement Section 43A of the PDPA.

1.6 Pursuant to the above, this Public Consultation Paper ("**PCP**") seeks to gather public views and feedback regarding aspects that will be or should be addressed in the proposed Data Portability Regulations and Data Portability Guideline.

PART 2: PROPOSED REQUIREMENTS FOR THE RIGHT TO DATA PORTABILITY

2.1 As an overview, Part 2 of this PCP on proposed requirements that will be addressed in the Data Portability Regulations and Data Portability Guideline is categorised as follows:

(a) Readiness for the right to data portability;

(b) Types of personal data subject to the right to data portability;

(c) Timeline to comply with data portability requests;

(d) Historical data;

(e) Fees; and

(f) Transmission of personal data arising from a data portability request.

[A] Readiness for the right to data portability

2.2 Background: The right to data portability can only be exercised and complied with where the transmission of personal data from the data controller to the receiving data controller is technically feasible.

2.3 "Technical feasibility" is defined as the ability of a data controller to effectively and efficiently transmit data from one data controller to another using available technology infrastructure and formats. Without technical feasibility, data controllers will not be able to comply with any data portability request since it would not be possible for the receiving data controller to receive or read any personal data transmitted by the data controller.

2.4 Nevertheless, it is recognised that achieving complete technical feasibility between all data controllers will be extremely costly to data controllers as it would require the implementation of new technical systems.

2.5 Other jurisdictions with the right to data portability such as the UK, EU and Thailand do not impose any requirements on data controllers to adopt or maintain processing systems that are technically feasible with those of other data controllers.

2.6 Proposal: It is proposed that data controllers will only be required to comply with data portability requests if there is technical feasibility between the data controller and receiving data controller.

2.7 Data controllers will not be required to adopt and maintain new systems or processes in order to achieve technical feasibility. However, data controllers will be required to comply with any common set of technical standards, data formats and specifications for data portability requests that have been specified by the:

(a) Commissioner; or

(b) data controller forum in respect of the sector / industry that it oversees.

2.8 Please note that any requirements imposed will only be imposed on data controllers within a certain sector/industry and will take into account the systems and processes

that are currently used by data controllers within that sector/industry. This is in order to prevent any disruption to or unnecessary costs being incurred by data controllers.

Question 1

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) What are your views on the preparedness of data controllers in relation to the introduction of the right to data portability for data subjects?

(b) What are the potential challenges that may be faced by data controllers when trying to comply with a data portability request?

(c) Where the Commissioner or data controller forum imposes specific requirements on technical standards, data formats and specifications, what are the potential challenges data controllers may face as a result of the imposition of these requirements?

(d) Are there currently any existing open access, interoperability or data portability-related initiatives in place in Malaysia? If your answer is yes, please provide details of such initiatives.

(e) Are there currently any common set of standards, data formats and technical standards that may be imposed on data controllers within a particular sector / industry? If your answer is yes, please specify the sector / industry you are referring to along with details of such standards, data formats and technical standards.

[B] Types of personal data subject to the right to data portability

2.9 Background: Other jurisdictions typically limit the right to data portability to only certain types of personal data. Jurisdictions such as the EU, UK, and Thailand typically limit this right to personal data that: (i) relates to the data subject; (ii) is in electronic form; (iii) was provided by the data subject to the data controller; and (iv) was collected and processed on the grounds of consent or for the performance of contract.

2.10 Proposals:

2.10.1 It is proposed that the right to data portability be limited to personal data that meet the following requirements:

(a) personal data that is directly provided by the data subject;

Examples:

Personal data provided directly includes data provided by the data subject when completing registration forms or other types of forms provided by the data controller. Personal data falling under this category include a data subject's names, email address and NRIC number.

This is distinct from "observed data" which refers to personal data that is collected through the data controller's direct observation of the behaviour of the data subject. This includes

website usage or search activities, traffic and location data and other raw data processed by connected objects such as smart meters and wearable devices.

(b) personal data processed based on consent (or explicit consent) or based on a contract to which the data subject is a party to;

(c) personal data processed by automated means. All personal data that are processed and stored manually (i.e. non-electronically) will not fall under this right to data portability; and

(d) personal data not classified as inferred data or derived data.

Examples:

"Inferred data" refers to any information or conclusion drawn about the data subject based on the analysis, patterns or correlation of other data about the data subject to ascertain certain characteristics or tendencies about the data subject without needing to obtain information directly from the data subject.

"Derived data" refers to any information about the data subject that is derived by the data controller by analysing, processing or aggregating other data about the data subject.

An important distinction is that both inferred and derived data are created / derived by data controllers through further processing of existing personal data. Examples include:-

- *the outcome of an assessment of the health condition of a data subject by a doctor;*
- *the creation by a financial institution of a profile for risk management and fulfilling financial regulations; and*
- *the personalisation of the content or types of advertisement provided to a data subject through user categorisation or profiling based on their behaviour and activities on social media.*

Inferred and derived data may be distinguished from observed data based on the following question:

"does the data in question exist as a result of any processing required to be carried out by the data controller or a data processor engaged by the data controller?"

When a data controller collects a person's Google search and web history, such data is considered to be observed data as it is a direct observation of a data subject's searches. Any data generated as a result of the processing of the search and web history (i.e. a data subject's behavioural analysis or ad preferences) will be considered to be inferred and derived data (this excludes any personal data provided directly by the data subject as provided in the example under Paragraph 2.10.1).

2.10.2 It is proposed that whitelists providing a list of personal data that are to be transmitted as part of a data portability request be employed. These whitelists will be issued by the Commissioner, data controller forum or regulator of each sector / industry for data controllers in each sector/industry, and will likely differ across sectors/industries. Data controllers will only be required to transmit data belonging to the categories listed in the whitelist. However, where a data subject requests for data that does not belong

to any category listed in the whitelist, data controllers may voluntarily transmit such data.

Question 2

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) Do you think the scope of the right to data portability is adequate? Should the scope be further expanded or limited? If so, in what ways?

(b) Do you think "observed data" should be included or excluded from the right to data portability?

(c) Do you think the exclusion of "derived data" and "inferred data" from the right to data portability may inadvertently exclude certain types of personal data that would benefit your right to data portability? If so, which types of data?

For example, a doctor's clinical notes would be considered as inferred data and therefore would be excluded from the right to data portability. Data subjects will not be able to utilise this right to request for the transmission of such data from one data controller to another.

(d) Do you believe that adopting a whitelisting approach in the Guidelines would help eliminate any potential ambiguity or confusion regarding the types of personal data that fall within the ambit of the right?

(e) If so, which types of personal data do you think should be included within the scope of such whitelist?

[C] Timeline to comply with data portability requests

2.11 Background: It is necessary to provide data controllers with a timeline to comply with when dealing with a data portability request. This timeline should not be too long as it could render the data portability request redundant particularly in cases where the receiving data controller needs the data urgently. However, it should not be too short as data controllers would require sufficient time to compile all relevant personal data for transmission.

2.12 Other jurisdictions such as the EU and UK typically require data controllers to comply with data portability requests within one (1) month from the date of receipt of the request. An extension of a further two (2) months is allowed for complex cases, provided that the data subject has been informed about the reasons for such delay within the initial first month of receipt of the request.

2.13 Proposal: It is proposed that data controllers be given 21 days to comply with a data portability request. In the event that they are unable to comply with the request within 21 days, they will be required to comply with the request no later than 14 days after the expiration of the initial 21-day period. This timeline is similar to that provided for data access and data correction requests.

Question 3

In providing your responses to the questions below, please provide clear justifications to support your views:

Is the timeline under the current proposal reasonable or should a shorter / longer timeline be given for data controllers to respond to data portability requests?

[D] Historical data

2.14 Background: A data controller will likely process and retain personal data that was previously collected. When a data subject exercises their right to data portability, data controllers may then be required to transmit all applicable personal data, including personal data that was previously collected and is still being retained by the said data controllers.

2.15 Please note however that the personal data retained by data controllers is still subject to the retention principle and must be permanently deleted or destroyed when the data controller no longer requires such data for its purposes or has no reason to retain the same, subject at all times to the applicable statutory retention periods.

2.16 Amongst the jurisdictions referenced, namely EU, UK, Singapore, Philippines, Indonesia and Thailand, there are no time limits on data portability requests in relation to personal data that has been collected and retained by data controllers.

2.17 Proposal: It is proposed that no time limits or limitation period be imposed on data portability requests in respect of personal data previously collected and being retained by data controllers.

Question 4

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) Should there be a time limit / limitation period imposed on data portability requests for personal data processed and retained by the data controller prior to the request?

(b) If your answer is yes, what should this time limit / limitation period be?

[E] Fees

2.18 Background: Data controllers may incur costs as a result of complying with data portability requests. These costs would take the form of expenses incurred, time and manpower spent in conducting searches for all relevant personal data, as well as for the transmission of such personal data to the receiving data controller.

2.19 The EU and the UK generally prohibit data controllers from charging any fees for responding to a data portability request. However, they are allowed to charge a reasonable fee if the request is manifestly unfounded or excessive. The fee charged should be reasonable and based on the administrative costs of complying with the request.

2.20 Proposal: It is proposed that data controllers be allowed to charge a fee for responding to data portability requests from data subjects to cover associated compliance costs. While data controllers do not have to prove that the requests are "manifestly unfounded or excessive", any fee imposed should only be based on the associated compliance costs. No profit may be earned from the imposition of this fee.

2.21 However, in order to ensure that any costs imposed are not excessive, it is proposed that a fee cap similar to that for data access requests is implemented to ensure fees are reasonable and affordable for data subjects while enabling data controllers to recover their related costs. This fee cap will be imposed by way of Regulation.

Question 5

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) Should data controllers be able to charge a fee for responding to data portability requests from data subjects to cover associated compliance costs?

(b) If no, please provide your reasons?

(c) If yes, please provide your reasons and state what the fee cap should reasonably be?

(d) What are your views on the fee cap varying based on the amount of data to be transmitted?

[F] Transmission of personal data arising from a data portability request

2.22 Background: Jurisdictions with the right to data portability such as UK, EU, Singapore, Thailand and the Philippines require personal data to be transmitted in a format which:

(a) supports re-use; and

(b) is in a structured, commonly used and machine-readable format.

2.23 In addition to the above, the EU and UK advise data controllers to adopt commonly used formats in the sector / industry that these data controllers operate in or, where no commonly used format is available, to adopt the use of open formats (i.e. XML, JSON, CSV).

2.24 Additionally, all jurisdictions with the right to data portability impose a responsibility on the data controller to ensure the safety of data during transmission and ensure that it is delivered to the correct destination.

2.25 Proposal: It is proposed that data controllers be provided with the flexibility to determine the best method available to transmit the requested data, provided that:

(a) the method of transmission complies with any common set of standards or data formats as specified by the Commissioner or relevant data controller forum; and

(b) there are appropriate security measures in place to ensure that the personal data is transmitted securely and to the correct destination / receiving data

controller. This includes meeting any minimum security requirements imposed by the Guidelines and security principle under Section 9 of the PDPA.

Question 6

In providing your responses to the questions below, please provide clear justifications to support your views:

(a) Do you agree that data controllers should have the flexibility to determine the method of transmission for data portability requests, as long as it complies with common standards and security measures?

(b) Are you aware of any existing common set of standards or data formats used by data controllers to share or transfer data? If yes, please state the necessaries.

(c) Are you aware of any existing sector / industry specific security requirements governing the transmission or sharing of data among data controllers, apart from the standards prescribed by the PDPA and Personal Data Protection Standard 2015? If yes, please state the necessaries.