ANNEX A

RESPONSE TO PDPC'S PUBLIC CONSULTATION
ON REVIEW OF THE PERSONAL DATA PROTECTION ACT 2012

PART II - PROPOSED DATA PORTABILITY OBLIGATION

Question 1
What are your views on the impact of data portability, specifically on consumers, market and economy?

Certis Comments:

From the perspective of a service provider, while we do recognise the potential and benefits of data portability, we are also concerned with the challenges that businesses like us are likely to face. These challenges include (i) ensuring the security and protection of the ported data; (ii) costs of implementation and compliance, especially for businesses that handle large volumes of data; (iii) managing risks arising from the transmission of data from one organisation to another and (iv) maintaining confidentiality of an organisation's competitiveness arising insights gleaned from the data. This will no doubt result in additional costs to service providers and even consumers in certain circumstances.

We think that a balance must be achieved between the interest of consumers and the costs of data portability to organisations. For this to happen, we propose that ported data be limited to data which are in the first provided by the individuals, and within a limited timeframe as set out in our commentary below.

Question 2
What are your views on the proposed Data Portability Obligation, specifically – a) scope of organisations covered; and b) scope of data covered?

Certis Comments:

We agree with the proposed scope of organisations covered, and that receiving organisations shall be limited to those that have a presence in Singapore.

However, we have some reservation on the scope of data covered. The proposed Data Portability Obligation would not be limited to personal data as defined in the PDPA. It would instead apply to data in the possession or control of organisations that is held in electronic form, regardless of whether it was originally collected in electronic or non-electronic form. Further, it also covers data that is provided by the user as well as data generated by the individual's activities in using the organisation's products or services.

Based on the above, the scope of data covered could become exceedingly broad and thereby increase the cost of compliance for organisations. For example, organisations that are in the process of digitising their physical records may subsequently find an even larger pool of covered data that is subject to compliance. As a result, organisations would be required to allocate more resources to fulfil the Data Portability Obligation.

Further, the inclusion of user activity data (in addition to user provided data) will significantly increase the burden on organisations. In this digital economy, large amounts of data are generated by the individual's activities but this data may or may not be actively utilized monitored by the organisation. As such, organisations will need to acquire the necessary systems and infrastructure to effectively monitor and manage the user activity data. This would undoubtedly result in greater costs for organisations - not only during the initial implementation but also in subsequent recurring maintenance and upgrading costs. We therefore suggest that the scope of data portability be limited to the personal data provided by the individual to the organisation.

As insights gleaned from user activities have competitive value to an organization such as enhancing user experience with the company, a company may spend on capital to capture certain data which it is of the view would provide it that competitive edge it requires for its business. We are of the view that such commercially sensitive data if disclosed, would reveal confidential commercial information that could harm the competitive position of the organisation. In this regard, we are also of the view that such data should be completely excluded from the Data Portability Obligation to protect the organisations' commercial interests and prevent distortion of competition. Such an approach would also be consistent with the proposal to exclude derived data from the Data Portability Obligations.

If PDPC is nonetheless minded to include user activity data as part of ported data, we suggest that the scope of user activity data subject to the Data Portability Obligation be further refined, for example by restricting it to a particular timeframe, so as to provide certainty to organisations. For instance, organisations could be only required to port user activity data generated in the past three months.

Even though organisations are allowed to charge a reasonable fee to recover the costs of providing data portability, it would be challenging for organisations to determine what is considered reasonable as it may vary depending on each case. Furthermore, this is not a straightforward process as there are multiple stages involved in handling and responding to data portability requests under the proposed Data Portability Obligations. Greater guidance on the fees payable would therefore be helpful to organisations seeking to implement such fees.

Question 4
What are your views on the proposed requirements for handling data portability requests?

Certis Comments:

The PDPC is proposing a period of no longer than 7 calendar days for data to be ported upon confirmation from the individual. We think that it may be very onerous for organisations to comply with a strict timeline, especially during the initial stages of implementation or when there is a surge in such requests.

To allow organisations to better cope with the requirements under the Data Portability Obligations, we urge the PDPC to consider adopting a more flexible approach as prescribed under the Access Obligation. Under the Access Obligation, an organisation is required to provide access as soon as reasonably practicable, and it shall inform the individual within 30 calendar days from the date of request if it is unable to comply.

PART III - PROPOSED DATA INNOVATION PROVISIONS

Question 7
What are your views on the proposed approach for organisations to use personal data for the specified businesses innovation purposes, without the requirement to notify and seek consent to use the personal data for these purposes?

Certis Comments:

Given the global trend towards increasing data privacy laws, there are concerns that growing regulatory and compliance pressure could stifle innovation and hinder the development of data analytics. We therefore welcome the PDPC's move to support the use of personal data for business innovation purposes.

We believe that the proposed changes are necessary and timely in today's data driven world. The gradual shift from consent as the preferred compliance strategy would encourage businesses to innovate and gain a competitive edge in the market. Amidst the rapidly evolving technological landscape, businesses should not be hindered by excessive regulation if the use of data can achieve business goals and bring about benefits for consumers.

However, it is unclear whether the proposed approach would apply to a data intermediary in relation to the personal data it processes on behalf of another organisation. If the organisation engages a data intermediary to process data on its behalf, we submit that the proposed provisions should similarly apply to the data intermediary.

For instance, ABC engages XYZ's services to deliver its products and provides XYZ with the details and addresses of the recipients. We are of the view that XYZ should be allowed to use

the data for purposes of operational efficiency and improving its services to ABC's customers without having to notify or seek consent for these purposes. Further, XYZ's existing obligations in relation to the protection and retention of the recipients' personal data would remain unchanged and unaffected.

We further note that the definition of business innovation purposes has been broadly worded in paragraph 3.3 of the consultation paper. For greater clarity, we suggest that the PDPC consider providing specific examples in addition to the illustration in paragraph 3.8.

Question 8
What are your views on the proposed definition of "derived data"?

Certis Comments:

We agree that derived personal data should be distinguished from such other derived data that cannot identify an individual, and that these two categories ought to be treated differently.

The proposed provisions clarified that consent is not required to use derived personal data for business innovation purposes. However, the consultation paper does not specify whether consent is required to disclose derived personal data to third parties in furtherance of such business innovation purposes.

For instance, in the event that third parties are engaged to develop new products and/or services for the organisation, it is submitted that the provisions should apply by extension to such third parties as well. The organisation will therefore not be required to obtain consent for the third party to receive and use the derived personal data only for the stipulated purpose.

Question 9.
What are your views on the proposal for the Access, Correction and proposed Data Portability Obligations not to apply to derived personal data?

Certis Comments:

While we are in favour and agree with the rationale for not subjecting derived personal data to certain existing Access and Correction Obligations, greater clarity should be made by PDPC on the scope of the exclusion as there may be inconsistency or incompatibility issues within the data regulation frameworks in Singapore and in other countries.

For example, organisations will still be required to provide (upon request) information about the ways in which the derived personal data has been or may have been used or disclosed by the organisation within a year before the date of the request, in accordance with Section 21(1)(b) of the PDPA. While, PDPC's suggestion of having a standard list of answers to the individual's

request is a good balance between the interests of customers and the constraints faced by businesses, it does not clarify the scope and limit of an organisation's obligation to response to individual's queries and requests. We are of the opinion that the provision of information on the purposes rather than the specific activities is a reasonable approach and should be clearly specified in the PDPA.

In relation to an individual's request to correct his or her personal data, the PDPC has proposed that organisations need not accede to request by individuals to correct derived personal data. As the accuracy and completeness of any data used in Artificial Intelligence (AI) led decision-making is of utmost importance, such an exception may result in adverse outcomes if derived personal data containing inaccurate data is allowed to be incorporated into AI algorithms and solutions. How can organisations reconcile the differences between the proposed exception and the data accountability-based practices set out in the PDPC's proposed Model Artificial Intelligence Governance Framework?