| UOB | | |
|---|---|---|
| **Section** | **Contents** | **UOB BN's Comments** |
| **3.1.1** | Under the PDPO, "personal data" is defined to mean "data, whether true or not, about an individual who can be identified (a) from that data; or (b) from that data and other information to which the organisation has or is likely to have access". | **Query # 1:**<br>The below are personal data that, on its own, can identify an individual: - Biometric identifiers (face geometry or fingerprints)<br>- Photograph or video image of an individual<br>- Voice of an individual<br>- DNA profile<br><br>As such, do the above personal data be applicable under PDPO? |
| | | Query # 2:<br>Would personal data that is generally available to the public (i.e. from websites which are accessible to the public – news portal, social media accounts which are open (i.e. not private)) be part of personal data exclusion? |
| | During public consultation briefing, social media accounts were mentioned as not included as part of PDPO but personal details such as name, telephone number, etc. obtained from individuals via social media should be treated as part of personal data. | **Query # 3:**<br>Would data given / disclosed via social media channels be subject to PDPO? |
| | | |
| **3.2.3** | As personal data which is of a more sensitive nature falls within the definition of personal data in the PDPO, it is subject to all the obligations in the PDPO. | **Query # 4:**<br>Para 3.2.2 stated that "However, the PDPO does not expressly recognise a distinction between sensitive and non-sensitive categories of personal data or define a category of "sensitive personal data". It is proposed that the PDPO applies across all types of personal data as a baseline, although sector-specific frameworks may address specific concerns relating to different types of data (e.g. financial data). ..."<br><br>If PDPO does not recognise or define distinction between sensitive and non-sensitive categories, would would then be considered as "personal data which is of more sensitive nature"? |
| | | |
| **4.5.1** | Under the Accountability Obligation in the PDPO, an organisation must appoint a person to be responsible for ensuring that it complies with the PDPO, typically referred to as a data protection officer ("DPO"); and develop and implement policies and practices that are necessary to meet its obligations under the PDPO, including a process to receive complaints. In addition, the organisation is required to communicate to its staff information about such policies and practices and make information available upon request to individuals about such policies and practices. | **Query # 5:**<br>Can International banks / organisations adopt and implement policies developed by parent / Head Office, provided obligations under local PDPO are adequately covered? |
| | | |
| **4.6.2** | Given that the type of consent could vary depending on the specific context of the collection, the manner in which consent may be given under the PDPO is not specifically prescribed. It is recognised that consent may be explicit or implied through an individual's actions or inaction, depending on circumstances. This gives organisations flexibility as to how they obtain consent. | **Query # 6:**<br>Following comment on recording of CCTV cameras as part of personal data, would a front door notice / sticker showing the premises has CCTV and it is being recorded be sufficient as a form of consent if the individual still proceed to enter the business premises. |
| | | |
| **4.6.4** | Deemed Consent: There are circumstances where consent may be deemed under the PDPO, broadly: | **Suggestion # 1:**<br>To consider adding circumstance whereby "*if the individual, does not object, when been afforded the opportunity to withdraw his consent at any time*" |
| | | |
| **4.6.4(b)** | if the collection, use or disclosure of the personal data is reasonably necessary for the conclusion of the contract between the individual and the organisation | **Suggestion # 2:**<br>To consider stating that consent is deemed where collection use or disclosure is reasonably necessary for **performance** of the contract, not just conclusion of the contract. |
| | | |
| **4.9.1** | Under the PDPO framework, individuals have the right to request an organisation to provide them with their personal data that is in the possession or under the control of the organisation, and information about the ways in which that personal data has been or may have been used or disclosed within a year before the date of request for access, subject to the exceptions in the PDPO. | **Suggestion # 3:**<br>Organisation be given an option of charging the individual a reasonable fee for complying with individual's access request (but not for correction request) in view of the costs involved in compliance with PDPO &/or recover incremental costs in responding to the access request.<br><br>**Suggestion # 4:**<br>A turnaround time frame to be stipulated for organisation to revert to the access request for proper management of both parties' obligations and expectations. Suggest a 30 working days period from date of such request with extension permissible as long as notification was provided within the 30 days. |
| | | |
| **4.9.2** | Individuals may also request for correction of their personal data or that their personal data be transmitted to another organisation, subject to certain exceptions in the PDPO. | As per **Suggestions # 3 and # 4** stated above. |
| | | |
| **4.14.1** | Under the PDPO, organisations are required to, as soon as practicable, but in any case, no later than 3 calendar days after making the assessment, notify the Responsible Authority of a data breach that:<br>(a) results in, or is likely to result, in significant harm to the individuals to whom any personal data affected by a data breach relates; or<br>(b) is or is likely to be, of a significant scale. | **Suggestion # 5:**<br>Suggest prescribed a list of data sets, where if such data is compromised, significant harm is deemed. This provides more certainty and objectivity.<br><br>**Suggestion # 6:**<br>Suggest "significant scale" be those that involve the personal data of 500 or more individuals, including if the actual number of affected individuals in a data breach is unable to be determined but is believed to be at least 500 during the initial assessment.<br><br>**Suggestion # 7:**<br>3 business / working days is more practical than 3 calendar days, taking into consideration the notification may need to be cleared at several levels and escalated to Senior Management for approval. |
| | | |
| **5.4.1** | Under the PDPO framework, individuals have the right to request an organisation to provide them with their personal data that is in the possession or under the control of the organisation, and information about the ways in which that personal data has been or may have been used or disclosed within a year before the date of request for access, subject to exceptions. This is also known as the "Access Obligation". | **Query # 7:**<br>Can organisation request for such request to be in orginal or acceptable verified written format only?<br><br>**Query # 8:**<br>Can organisation request individual to provide purpose of request for better and more appropriate scope of coverage? For e.g. if it is for credit application purpose, then organisation shall provide bank and/or loan statements in possession. |
| | | |

| | | |
|---|---|---|
| **5.4.8** | If the organisation rejects the individual's access request, it must notify the individual of the rejection within the prescribed time and in the prescribed manner. If the organisation has excluded personal data from the access request, it must notify the individual of the exclusion. | **Suggestion # 8:**<br>To define "prescribed time" and "prescribed manner".<br><br>**Query # 9:**<br>Does organisation need to provide reason for rejection base on the provided situations stipulated under para 5.4.7 of PDPO? |
| | | |
| **5.6.2** | When an individual submits a data porting request, the porting organisation is required to transmit the applicable data to the receiving organisation in the prescribed manner if certain conditions are fulfilled. The data porting request must satisfy the prescribed requirements and there must be an ongoing relationship between the individual and the porting organisation. | **Suggestion # 9:**<br>To facilitate data transfer, suggest the "applicable data" can be industry specific and curated for the nature of services. |
| | | |
| **8.1** | The PDPO may provide for the establishment of a DNC regime. Individuals may request for their telephone numbers to be added to the DNC Registry if they do not wish to receive telemarketing messages via phone call, text message (i.e. SMS, MMS or any electronic communications sent using a telephone number, e.g. WhatsApp, Telegram) or fax. The DNC Registry will be administered by the Responsible Authority. | **Suggestion # 10:**<br>Though DNC does not cover telemarketing messages via electronic emails, organisations should allow individuals to withdraw consent of such marketing emails which is common practice in other jurisdictions whereby there's "unsubscribe" link in such emails. |