

Annex D

May 2014

FACTSHEET

Extracts and Examples Adapted from the Advisory Guidelines for the Real Estate Agency and Telecommunication sectors; Key Concepts on Access, Correction and Overseas transfer of personal data; and Data activities relating to minors

(1) Advisory Guidelines on Key Concepts (on Access, Correction and Overseas Transfer of Personal Data)

Response time frame for access and correction requests

An organisation should respond to an access or correction request within 30 days. If an organisation is unable to respond to an access or correction request within 30 days from the time the request is made, the organisation shall inform the individual in writing within that time frame of the next soonest possible time¹ by which it will be able to respond to the request. It would be good practice for the organisation to also specify the reasons for not being able to respond within 30 days of receiving the requests. In general, if the organisation requires the individual to pay a fee in relation to an access request, the organisation should inform the individual of the fee amount (and all relevant details, e.g. accepted payment methods and payment processing time) when the organisation has obtained sufficient information to estimate the fee.

The Transfer Limitation Obligation

The PDPA limits the ability of an organisation to transfer personal data outside Singapore. In particular, the PDPA provides that an organisation must not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the PDPA to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA.

Conditions for transfer of personal data overseas

The Data Protection Regulations specify the conditions under which an organisation

¹ Organisations are reminded of the requirement to respond to an access request as soon as reasonably possible under section 21(1) and to make a correction as soon as practicable under section 22(2).

may transfer personal data to a recipient overseas. In essence, an organisation may transfer personal data to a recipient overseas if the transferring organisation reasonably believes, or has taken reasonable steps to ensure, that the recipient is bound by legally enforceable obligations to provide to the personal data transferred a standard of protection that is comparable to that under the PDPA.

In this regard, legally enforceable obligations include obligations imposed on the recipient under legal instruments such as:

- a) any law;
- b) any contract that requires the recipient to provide to the personal data transferred to the recipient a standard of protection that is at least comparable to the protection under the PDPA; or
- c) any binding corporate rules that require every recipient (that is related to the transferring organisation)² of the transferred personal data 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.

An organisation transferring personal data overseas is taken to have satisfied the abovementioned conditions for overseas transfer under circumstances such as:

- a) the individual whose personal data is to be transferred voluntarily gives his consent to the transfer of his personal data³;
- b) the transfer is necessary for the performance of a contract between the organisation and the individual. For example, Karen purchases an overseas tour with travel agency DEF. In order to perform its obligation under its contract with Karen to make the necessary hotel reservations, travel agency DEF is required to transfer her personal data (such as her name, nationality and passport number) overseas to the hotels that Karen will be staying at during the tour. Travel agency DEF's transfer of Karen's personal data in this case would be in compliance with the Transfer Limitation Obligation as it is necessary for the performance of the contract between travel

² For example, a subsidiary of the transferring organisation.

³ In order to rely on consent given by the individual, the organisation should (among other things) provide the individual with a reasonable summary of the extent to which the personal data transferred to those countries and territories is protected to a standard comparable to the protection under the PDPA.

agency DEF and Karen;

- c) the transfer is necessary for a use or disclosure in certain situations where the consent of the individual is not required under the PDPA, such as use or disclosure necessary to respond to an emergency that threatens the life, health or safety of an individual;
- d) the personal data is data in transit; or
- e) the personal data is publicly available in Singapore.

(2) Advisory Guidelines on Data Activities Relating to Minors

When can a minor give valid consent on his own behalf under the PDPA?

The PDPA does not specify the situations in which a minor (that is, an individual who is less than 21 years of age) may give consent for the purposes of the PDPA. In general, whether a minor can give such consent would depend on other legislations and the common law.

It is noted that the ages at which minors may conduct different types of activities on their own or are accorded certain legal protections vary across various local legislation⁴. In particular, the Civil Law Act provides that a contract entered into by a minor who has attained the age of 18 years has effect as if he was of full age (that is, 21 years of age), except as otherwise provided in that section or any other written law. Hence if a minor who is 18 years old or older gives consent to the collection, use or disclosure of his personal data in such a contract (and there are no other factors affecting the minor's legal capacity to enter into such a contract), such consent would generally be valid for the purposes of the PDPA.

For situations where there is no legislation that affects whether a minor may give consent, the issue would be governed by the common law. In this regard, PDPC notes that there is no international norm on when minors may exercise their own

⁴ Provisions that set out age thresholds for the purpose of according certain legal protections to minors include:

- a) The Employment Act (Cap. 91) defines a child as one below 15 years of age and a young person as one between 15 and 16 years of age for the purposes of according varying protections in respect of the different age groups; and
- b) The Children and Young Persons Act (Cap. 38) defines a child as one who is below 14 years of age and a young person as one that is between 14 and 16 years of age for purposes of according varying protections under that Act.



PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

rights under data protection laws. PDPC understands that in some countries, some kind of test of maturity is applied, taking into account factors such as the level of maturity of the minor, the minor's capacity to understand the nature of legal rights and whether there is any undue influence exerted on the minor, to determine if a minor can exercise legal rights. In addition, some countries have enacted legislation to specifically protect minors below a certain age. For example, in the United States, the Children's Online Privacy Protection Act ("COPPA") requires certain organisations to obtain verifiable parental consent to collect personal data from children under 13 years of age⁵.

PDPC notes that the age threshold of 13 years appears to be a significant one in relation to according protection to minors. For example, under the Employment Act, a child 13 years of age or older may be employed in light work suited to his capacity in a non-industrial undertaking and no child who is below the age of 13 years shall be employed in any occupation. Similarly, some film and video classification ratings set out age thresholds for audiences for such content, including Parental Guidance 13 ("PG13"). In addition, organisations that face exposure to COPPA (e.g. companies that provide online services to individuals in the US) may also already have policies and procedures that are premised on the age threshold of 13 years in relation to consent to the collection, use and disclosure of their personal data.

PDPC is of the view that organisations should generally consider whether a minor has sufficient understanding of the nature and consequences of giving consent, in determining if he can effectively provide consent on his own behalf for purposes of the PDPA. It is also noted that, as a practical matter, some organisations may already have policies or practices providing for an age threshold of 13 years in relation to consent. Bearing this in mind, PDPC will adopt the practical rule of thumb that a minor who is at least 13 years of age would typically have sufficient understanding to be able to consent on his own behalf. However, where, for example, an organisation has reason to believe or it can be shown that a minor does not have sufficient understanding of the nature and consequences of giving consent, the organisation should obtain consent from an individual, such as the minor's parent or guardian, who is legally able to provide consent on the minor's behalf.

Example 1: Consent on own behalf

⁵ See, for example: <http://www.ftc.gov/news-events/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over>

A 19-year-old signs up for a subscription to a magazine. The subscription contract also obtains consent from him for the collection, use or disclosure of personal data by the publisher of the magazine for the purpose of marketing its other magazines. Generally, he would be considered to have given consent under the PDPA for this purpose on his own behalf.

Example 2: Obtaining consent from parent/legal guardian

A pre-school wishes to organise a field trip to a zoo for its students. It needs to disclose participants' personal data to the zoo for the purpose of arranging the field trip's programme.

Generally, the pre-school should obtain consent from the parent or other legal guardians of each student, as a pre-school student would not have legal capacity to give consent.

(3) Advisory Guidelines for the Real Estate Agency Sector

Example 1: Marketing of potential en-bloc sale

Estate agent ABC is assisting the Management Corporation ("MC") of a condominium to market a potential en-bloc sale of the condominium to owners of units in the condominium.

ABC has compiled a list containing the names, addresses and telephone numbers of owners taken from various sources including online title search services, the MC and communications with neighbours of some of the owners. ABC intends to first contact the owners by mailing letters to inform them of the potential en-bloc sale, and then place follow-up calls to these owners.

In this case, the Data Protection Provisions will apply as ABC has collected and used personal data relating to the individual owners to market the potential en-bloc sale. Among other things, ABC will have to obtain consent from the individual owners on or before collecting and using their personal data, unless exceptions apply. In this regard, possible exceptions may include if the personal data is publicly available.

(4) Advisory Guidelines for the Telecommunication Sector

Example 1: Inclusion of advertisements with bills



PERSONAL DATA
PROTECTION COMMISSION
S I N G A P O R E

PDPC understands that telecommunication operators may include advertisements for specific products or services as inserts in bills addressed to individuals or in the form of promotional messages printed on the bills themselves.

Where a telecommunication operator packages such advertisements together with bills that are addressed to an identifiable individual (whether as an insert, or as a message printed on the bills themselves), the telecommunication operator would generally be considered to have used personal data for advertising purposes, even if the advertisements themselves are not addressed to the individual. Correspondingly, the Data Protection Provisions would apply to such use. Among other things, when an individual withdraws consent under the PDPA for such purposes, the telecommunication operator would be required to allow and facilitate such withdrawal. The Key Concepts guidelines contain more details of the actions to be taken when receiving a notice of withdrawal of consent.

For media queries, please contact:

Mr Kenneth Tan
Manager, Media Relations, Personal Data Protection Commission
Tel: 6211 1600
E-mail: kenneth_tan@pdpc.gov.sg