PDPC UPDATE ON ANONYMISATION AND HEALTHCARE

The Personal Data Protection Commission (**PDPC**) has recently updated the following guidelines:

(1) Advisory Guidelines for the Healthcare Sector
(2) Advisory Guidelines on Selected Topics – the changes made were solely in section 3, the chapter on anonymisation

A brief summary of the updates and changes is set out below.

(1) **Advisory Guidelines for the Healthcare Sector ("Healthcare Guidelines")**

The Healthcare Guidelines have been updated to provide clarity on the sending of service reminders by healthcare organisations to their patients.

Service reminders, such as appointment reminders, are typically not considered "specified messages" if the sole purpose of such messages was to remind patients of appointments and other messages related to the managing of the doctor-patient relationship.

Three new examples have been added to illustrate this point:

The Healthcare Guidelines have been updated to provide clarity on the sending of service reminders by healthcare organisations to their patients.

Example 1 – using personal data collected before the appointed day for sending reminder messages

Dental Clinic ABC collected John's personal data before 2nd July 2014 and has been sending him reminders by post to visit the dental clinic. Hitherto, John has not withdrawn consent nor has he indicated that he does not consent to such use of his personal data.

Dental Clinic ABC may continue to send such reminders to John until he indicates that he no longer wishes to receive them.

Example 2 – sending of reminder messages generally

James visits Dental Clinic DEF for the first time for a dental treatment. At the end of the visit, James makes an appointment with Dental Clinic DEF for his next visit. A week before the appointment date, Dental Clinic DEF sends James a text message at his Singapore telephone number solely to remind him of his appointment.

Such a reminder sent by Dental Clinic DEF solely for the purpose of reminding James of his appointment would unlikely be considered a specified message.

Example 3 – obtaining clear and unambiguous consent

Jason visits Dental Clinic DEF for the first time for a dental treatment. When providing his personal data to Dental Clinic DEF in the patient registration form, Jason checks a box to indicate that he consents to receiving reminder text messages from Dental Clinic DEF for subsequent dental visits.

Jason would be considered to have provided clear and unambiguous consent for Dental Clinic DEF to send reminder text messages for his next dental visits. Dental Clinic DEF may send such messages to Jason without checking the Do Not Call Registry.

Examples 1 and 2 serve to emphasise that the sending of reminder and service messages solely for the purpose of reminding patients about matters such as their appointments would **not** be considered the sending of a specified message.

Example 3 however, is unusual as it seems to contradict Examples 1 and 2 and suggest that:

i) reminder text messages **are** specified messages; and
ii) clear and unambiguous consent **is** required to send reminder text messages to patients.

This directly contradicts Examples 1 and 2 as well as the general framework and understanding of the Do-Not-Call Provisions.

The Do-Not-Call Provisions regulate the sending of "specified messages" which includes, among others, messages which are intended to "offer to supply goods or services or to advertise or promote goods or services etc."

A service message sent solely to remind a patient about their appointments, such as the one described in Examples 1 and 2, would not come within the definition of "specified message" and should not be regulated under the Do-Not-Call Provisions.

Based on Examples 1 and 2, the guidance provided in the Healthcare Guidelines and the definition of "specified message" under the Do-Not-Call Provisions, it should still be the case that messages which are **solely** service messages would not be considered "specified messages", and clear and unambiguous consent would therefore not be required to send such messages.

(2) **Advisory Guidelines on Selected Topics – the changes made were solely in section 3, the chapter on anonymisation ("Anonymisation Chapter")**

The updated guidelines provide greater clarity on organisations in their use and disclosure of anonymized data, and provide more detail on the issues which organisations should consider when carrying out anonymisation of personal data.

The new points of clarity and guidance are highlighted in brief below:

(a) **What is "anonymisation"?**

The PDPC is aware that different jurisdictions understand the term "anonymisation" to mean different things, and has provided clarity on what they consider "anonymisation" to be:

> *The term 'anonymisation' refers to the process of converting personal data into data that cannot be used to identify any particular individual, and can be reversible or irreversible. The reversibility of the specific process used would be a relevant consideration for organisations when managing the risk of re-identification.*

The PDPC has also emphasized that personal data would not be considered anonymized if there is a serious possibility that an individual can be re-identified, having regard to:

i) the data itself, or the data combined with other information to which the organisation has or is likely to have access; and
ii) the measures and safeguards (or lack thereof) implemented by the organisation to mitigate the risk of identification.

Conversely, the PDPC has also stated that an organisation would generally be considered to have anonymised data if there is no serious possibility that a data user or recipient would be able to identify any individuals from that data.

(b) **Considerations when anonymising data – can the data be effectively or meaningfully anonymised?**

Having regard to the above, organisations should also bear in mind the fact that not all datasets can actually be effectively or meaningfully anonymised. The PDPC in its updated section on anonymisation has elaborated on some of issues which organisations should consider when anonymising data. These are set out below.

i) Nature and type of data

If the nature of the personal data is such that it is inherently full of information (e.g. a portrait photograph), anonymisation of the photograph is possible. However, effective anonymisation of the portrait photograph may render the photograph useless for its intended purpose.

In addition, the more unique a particular dataset, the more difficult it will be to effectively anonymise that dataset as the risk of re-identification will also correspondingly increase.

ii) Potential impact on individuals

In deciding whether to anonymise personal data for use or disclosure, organisations should

also consider any potential negative impact on individuals if they were to be re-identified (e.g. records of individuals with HIV records).

In situations where the organization is handling such sensitive personal data, even if the organization assesses that there is a less than serious possibility of the individual being identified from the anonymised data, the organization should still exercise caution and care when using and disclosing such anonymised data.

(c) **Considerations when anonymising data – is there a risk of re-identification?**

i) Nature of use and extent of disclosure

The nature of use and extent of disclosure can affect the risk of re-identification. For example, whether the organization uses the anonymised data within the organization itself or discloses it for use to all users generally - as the number of people having access to the data increases, the chances of re-identification also increases.

ii) Public knowledge and personal knowledge

The organization should consider the types of information that could enable re-identification if combined with the anonymised data, as well as the ease with which such information can be accessed. The organization can then tailor and implement an appropriate set of risk management controls for the intended use and the intended recipients of such data.

If, for example, it is known or foreseeable that the data may be accessed by individuals with special knowledge that could be used to re-identify individuals from that data, this risk must be accounted for in the risk assessment exercise.

iii) Disclosing multiple datasets

If an organization intends to disclose multiple anonymised datasets, the organization should also carry out an assessment of the risk of re-identification, especially if the datasets are extracted from the same database. There is a risk that a combination of these anonymised individual datasets may enable recipients to re-identify the individuals.

iv) Data recipient's ability and motivation to re-identify

The organisation should also consider the data recipient's ability to re-identify the individuals (e.g. the tools at their disposal) as well as whether there are any disincentives to re-identification (e.g. contractual obligations or regulatory consequences).

v) The changing environment and the increasing likelihood of re-identification

Even if a dataset may be anonymised at a particular point in time, it is not guaranteed that a

dataset will stay anonymised permanently. The likelihood of re-identification for any given anonymised dataset is likely to increase over time, due to greater ease of access to and volume of other relevant information, increase in computing power and improvements in data-linking techniques.

With technological advancements, a dataset that is sufficiently anonymised based on current technology might be more easily re-identified.

Considering the speed of technological advancements in this day and age, the PDPC has emphasised that it is important to build in robust organisational, legal and non-technical measures to manage the risk of re-identification. It is also important for organisations to consider if a periodic re-assessment of re-identification risks should be included as a safeguard.

(d) **Assessing the risk of re-identification**

Proper management of re-identification risks reduces the likelihood that anonymised data will be re-identified in the future.

An assessment of the risks of re-identification should include an assessment of all the risk management controls that are applicable to the recipient organisation, including the technical, legal, regulatory and organisation measures. Examples of some of the measures which an organisation can consider putting in place to lower the risk of re-identification include:

i) limiting the number of data recipients to whom the information is disclosed and the number of persons that can access the information;
ii) imposing restrictions on the data recipient on the use and subsequent disclosure of the data;
iii) requiring the data recipient to implement processes to govern the proper use of the anonymised data in line with the restrictions;
iv) requiring the data recipient to implement processes and measures for the destruction of data as soon as the data no longer serves any business or legal purpose;
v) putting in place controls to limit the data users' or recipients' access to information that could assist in re-identifying the anonymised data (this may be difficult to implement in practice, especially if large amounts of anonymised data from the same databases are already publicly available).

The PDPC has also helpfully provided some scenarios to illustrate how the re-identification risks can be assessed and managed in certain circumstances.

i) Use of anonymised data within the organisation

If departments within an organisation have, or are likely to have, access to other information (e.g. the decryption key or algorithm to reverse the anonymisation process) that can be combined with the data to re-identify the individual, then that data will be considered personal data and the data protection provisions of the PDPA will apply.

The PDPC acknowledged that there may be circumstances where an organisation would like to convert personal data into anonymised datasets to be used for a particular purpose, but still needs to retain the original dataset in identifiable form. Here, the PDPC has stated that the organisation should establish effective barriers to access (e.g. user access controls, contractual terms) by the department using the anonymised data and the department holding the decryption key or other information that could be used to re-identify the dataset.

ii) Disclosure of anonymised data to a specific group (or groups) or data recipients

Where an organisation anonymises personal data in order to disclose it to a group of recipients, the organisation may continue to have access to other information that can re-identify the individual.

In such instances, the organisation should consider adopting appropriate measures to discourage attempts by data recipients from re-identifying the individuals (e.g. contractual safeguards).

(e) **Type of anonymisation technology to apply to the data**

The PDPC has stated that it is not necessary to apply the most technically sophisticated anonymisation technology to the data.

However, organsiations should apply anonymisation technology that is sufficiently robust to manage the risk of re-identification, having regard to all the circumstances, including:

i) The extent of the disclosure;
ii) The intended recipients (and number of recipients);
iii) Any existing controls over the disclosure of the data.

If you would like information on this or any other area of law, you may wish to contact the partner at WongPartnership that you normally deal with or contact the following lawyer:

LAM Chung Nian
Head – Intellectual Property, Technology and Media
Telecommunications and Data Protection Practices
DID: +65 6416 8271
Email: chungnian.lam @wongpartnership.com
Click here to see Chung Nian's CV.

Jeffrey LIM
Partner – Intellectual Property, Technology and Media
Telecommunications and Data Protection Practices
DID: +65 6416 8250
Email: jeffrey.lim @wongpartnership.com
Click here to see Jeffrey's CV.

WONGPARTNERSHIP OFFICES

SINGAPORE

WongPartnership LLP
12 Marina Boulevard Level 28
Marina Bay Financial Centre Tower 3
Singapore 018982
Tel: +65 6416 8000
Fax: +65 6532 5711/5722

CHINA

WongPartnership LLP
Beijing Representative Office
Unit 3111 China World Office 2
1 Jianguomenwai Avenue, Chaoyang District
Beijing 100004, PRC
Tel: +86 10 6505 6900
Fax: +86 10 6505 2562

WongPartnership LLP
Shanghai Representative Office
Unit 1015 Corporate Avenue 1
222 Hubin Road
Shanghai 200021, PRC
Tel: +86 21 6340 3131
Fax: +86 21 6340 3315

INDONESIA

Makes & Partners Law Firm
(an associate firm)
Menara Batavia, 7th Floor
Jl. KH. Mas Mansyur Kav. 126
Jakarta 10220, Indonesia
Tel: +62 21 574 7181
Fax: +62 21 574 7180
Website: makeslaw.com

MALAYSIA

Foong & Partners
Advocates & Solicitors
(an associate firm)
13-1, Menara 1MK, Kompleks 1 Mont' Kiara
No 1 Jalan Kiara, Mont' Kiara
50480 Kuala Lumpur, Malaysia
Tel: +60 3 6419 0822
Fax: +60 3 6419 0823
Website: foongpartners.com

MIDDLE EAST

Al Aidarous International Legal Practice
(an associate firm)
Abdullah Al Mulla Building, Mezzanine Suite 02
39 Hameem Street (side street of Al Murroor Street)
Al Nahyan Camp Area
P.O. Box No. 71284
Abu Dhabi, UAE
Tel: +971 2 6439 222
Fax: +971 2 6349 229
Website: aidarous.com

Al Aidarous International Legal Practice
(an associate firm)
Zalfa Building, Suite 101 - 102
Sh. Rashid Road
Garhoud
P.O. Box No. 33299
Dubai, UAE
Tel: +971 4 2828 000
Fax: +971 4 2828 011

MYANMAR

WongPartnership Myanmar Ltd.
No. 1, Kaba Aye Pagoda Road
Business Suite #03-02, Yankin Township
Yangon, Myanmar
Tel: +95 1 544 061

contactus@wongpartnership.com **wongpartnership.com**