Data Protection Quarterly Updates (October – December 2023)

The Personal Data Protection Commission (**PDPC**) published three decisions between October and December 2023 after concluding the following investigations:

(a) One investigation relating to the Purpose Limitation Obligation (as described below) under the Personal Data Protection Act 2012 (**PDPA**); and

(b) Two investigations relating to the Protection Obligation (as described below) under the PDPA.

The following table summarises the directions imposed in each of the decisions:

Name of decision	Relevant Obligation(s)	Decision and directions imposed
Tipros [2023] SGPDPC 7	Purpose Limitation Obligation	Direction issued to: (a) remove complainant's personal data from public platform; and (b) review other posts containing other individuals' personal data and remove such personal data if disclosure is not reasonable or proportionate.
Ascentis Pte. Ltd. [2023] SGPDPC 10	Protection Obligation	Financial penalty of $10,000. No further directions issued on account of remedial measures already taken.
Tokyo Century Leasing (Singapore) Pte. Ltd. [2023] SGPDPC 9	Protection Obligation	Financial penalty of $82,000. No further directions issued on account of remedial measures already taken.

The PDPC also published two practical guidances to Zuellig Pharma and Meta which covered issues relating to transfers of personal data for the purposes of providing a privacy enhancing technology solution and anonymised data.

© WongPartnership LLP
DISCLAIMER: This update is intended for your general information only. It is not intended to be nor should it be regarded as or relied upon as legal advice. You should consult a qualified legal professional before taking any action or omitting to take action in relation to matters discussed herein.
WongPartnership LLP (UEN: T08LL0003B) is a limited liability law partnership registered in Singapore under the Limited Liability Partnerships Act 2005.

Tipros [2023] SGPDPC 7

Comments

This decision emphasises the need for organisations to exercise discretion when responding to customer comments or complaints on public platforms, especially if the organisation intends to disclose personal data in its response.

As a matter of prudence, organisations may wish to refrain from disclosing their customers' personal data on public platforms unless absolutely necessary.

Facts

Tipros was a sole proprietorship in the business of wholesale and repair of electrical appliances. The complainant was a customer of Tipros who gave it a "1-star" review on Google reviews.

In its response to the complainant's review, Tipros included the complainant's personal data, including her residential address and mobile number. The PDPC found 13 other responses on Tipros' Google reviews page which disclosed, in similar fashion, personal data of other customers who had given reviews.

Decision

The Purpose Limitation Obligation requires organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances, and to inform the individual of the same prior to such collection, use or disclosure.

The PDPC held that, when an individual chooses a public platform to comment on an organisation, the organisation is entitled to respond on the same platform in a proportionate and reasonable manner. In particular, where the individual invites the organisation to advance an explanation, it may be necessary for the organisation to use or disclose relevant facts for such explanation to be effective. The PDPC held that such disclosure would be reasonable provided that the extent of disclosure is proportionate.

Further, the PDPC held that, where an individual makes a complaint on a public platform regarding an organisation, and it is necessary for the organisation to use or disclose personal data to respond with an explanation, then the individual would be deemed to have been informed prior to such use or disclosure since he or she had elicited the response.

In this case, the PDPC held that Tipros' disclosure of personal data was unreasonable and disproportionate. This is because the complaint related to the poor standard of service delivered by Tipros, and no issues were raised as to the location for delivery of the service.

© WongPartnership LLP
DISCLAIMER: This update is intended for your general information only. It is not intended to be nor should it be regarded as or relied upon as legal advice. You should consult a qualified legal professional before taking any action or omitting to take action in relation to matters discussed herein.
WongPartnership LLP (UEN: T08LL0003B) is a limited liability law partnership registered in Singapore under the Limited Liability Partnerships Act 2005.

Accordingly, the PDPC issued directions for Tipros to remove the disclosure of the complainant's residential address and mobile number on its Google reviews page, as well as to review the 13 other responses where it had also disclosed personal data of other customers. If such disclosure was not reasonable or proportionate for the purpose of responding to the Google reviews, Tipros is to remove such disclosure.

A copy of this decision may be accessed here.

Ascentis Pte. Ltd. [2023] SGPDPC 10

Comments

This decision serves as a timely reminder that when engaging data intermediaries, organisations should assess whether the data protection requirements they impose on such data intermediaries are sufficiently specific and comprehensive, taking into account the volume and sensitivity of personal data involved.

As demonstrated in this decision, it may not, for the purpose of complying with the Protection Obligation, be sufficient to merely impose on data intermediaries broad data protection obligations and/or a general obligation to comply with the standards of personal data protection under the PDPA.

Facts

Ascentis Pte. Ltd. (**Ascentis**) was a software company engaged by Starbucks Coffee Singapore Pte Ltd (**Starbucks SG**) to develop, implement, support, and host a Customer Relationship Management System (**CRM System**) to support a loyalty programme (**Rewards Program**).

Starbucks SG also separately engaged Ascentis to develop and provide technical support for an online store for the sale and purchase of products by Starbucks SG (**Platform**).

To provide additional support for the execution of this project, Ascentis engaged Kyanon Digital Co. Ltd (**Kyanon**), a software company in Vietnam. Employees of Kyanon were provided with accounts to the Platform with full administrative privileges.

In May 2022, a Kyanon employee left the employ of Kyanon and handed over the credentials for his administrative account (**Ex-Employee Account**) to the remaining members of the team *via* a shared Google Sheet. The account was not disabled thereafter. Instead, Kyanon employees changed the password of his account, updated the shared Google Sheet with the new password, and continued using the account among themselves.

In September 2022, a malicious threat actor used the Ex-Employee Account to gain access to the Platform, where personal data of certain Rewards Programme members was stored. As a result, the personal data of 332,774 individuals, including names, email addresses, physical addresses and telephone numbers (**Subject Data**) was exfiltrated.

© WongPartnership LLP
DISCLAIMER: This update is intended for your general information only. It is not intended to be nor should it be regarded as or relied upon as legal advice. You should consult a qualified legal professional before taking any action or omitting to take action in relation to matters discussed herein.
WongPartnership LLP (UEN: T08LL0003B) is a limited liability law partnership registered in Singapore under the Limited Liability Partnerships Act 2005.

Decision

Under the Protection Obligation, an organisation is required to protect personal data in its possession or under its control by making reasonable security arrangements. This obligation also applies to data intermediaries.

As a data intermediary of Starbucks SG, Ascentis was subject to the Protection Obligation in relation to the Subject Data. The PDPC found, having regard to the large volume of personal data hosted on the Platform, that reasonable security arrangements to protect the Subject Data were not implemented.

First, Ascentis failed to disable the Ex-Employee Account after Kyanon's ex-employee was no longer working on the project, and instead permitted its continued use by the remaining Kyanon employees.

Second, the Ex-Employee Account was not protected with a sufficiently complex password. After taking over the Ex-Employee Account, Kyanon employees changed the password to "Kyanon@123456". While this met the Platform's password complexity requirements, the PDPC reiterated that mere technical compliance with password complexity requirements is not good enough if the password remains guessable.

Third, the PDPC also found that the sharing of credentials for the Ex-Employee Account *via* a shared Google Sheet meant that anyone who obtained access to the said Google Sheet could gain access to the Ex-Employee Account. This heightened the risk of unauthorised access, especially if a malicious actor was familiar with the user identity of the Ex-Employee Account.

While the weak password and insecure sharing of account credentials were caused by Kyanon employees, the PDPC held that Ascentis could have specified clearer data protection requirements to Kyanon, including in relation to account management.

In this regard, the PDPC noted that, while the Master Services Agreement between Ascentis and Kyanon imposes broad data protection obligations, it did not mandate any specific measures in relation to account management. In addition, while Kyanon signed a Letter of Undertaking in which it undertook to comply with the standards under the PDPA and certain security and personal data policies, both the Letter of Undertaking and Master Services Agreement did not set out any specific requirements for disabling ex-employee accounts.

The PDPC separately observed that two other data protection practices could have prevented the unauthorised disclosure of personal data in this instance. In particular, multi-factor authentication (**MFA**) should be implemented as a baseline requirement for administrative accounts with access to confidential or sensitive personal data or large volumes of personal data. Organisations should also review user accounts to ensure that only necessary rights are assigned.

In the circumstances, the PDPC imposed a financial penalty of $10,000 on Ascentis. It noted that the personal data of 332,774 individuals was affected and that such data consisted largely of basic contact and account membership information. It also recognised that Ascentis had been cooperative, had taken prompt remedial actions, and had not previously been found to have breached the PDPA.

A copy of this decision may be accessed here.

© WongPartnership LLP
DISCLAIMER: This update is intended for your general information only. It is not intended to be nor should it be regarded as or relied upon as legal advice. You should consult a qualified legal professional before taking any action or omitting to take action in relation to matters discussed herein.
WongPartnership LLP (UEN: T08LL0003B) is a limited liability law partnership registered in Singapore under the Limited Liability Partnerships Act 2005.

***Tokyo Century Leasing (Singapore) Pte. Ltd.* [2023] SGPDPC 9**

Comments

This decision highlights that organisations should ensure that issues concerning software patch management and monitoring are properly addressed in their arrangements with external information technology (**IT**) vendors. In particular, organisations should not assume that their IT vendors would assume responsibility of conducting checks for patches and updates unless this has been expressly set out in the relevant contractual documentation.

Facts

Tokyo Century Leasing (Singapore) Pte. Ltd. (**TCL SG**) was a leasing and hire-purchase business which operated a website through which customers could submit applications to enter into hire-purchase or leasing agreements.

On 14 June 2022, TCL SG discovered that seven servers and six employee computers had been infected with ransomware. This resulted in the encryption of the personal data of 141,412 individuals, including national registration identity card (**NRIC**) numbers, income statements, email addresses and bank accounts (**Subject Data**).

Following investigations conducted by the PDPC and an IT forensics investigation firm, it was revealed that the software installed on a firewall device used by TCL SG was an outdated version and had a known vulnerability. The most likely cause of the incident was that malicious actor(s) had exploited this vulnerability to gain access to TCL SG's virtual private network.

The manufacturer of the firewall device released a patch in May 2019 to address the vulnerability, but it had not been installed at the time of the incident.

Decision

Under the Protection Obligation, an organisation is required to protect personal data in its possession or under its control by making reasonable security arrangements.

The PDPC held that TCL SG failed to implement reasonable security arrangements to protect the Subject Data for the following reasons.

First, TCL SG did not conduct regular monitoring of software patches for the software installed on the firewall device. The device had been in use since September 2019, more than three months since the patch was released. The vulnerability remained un-patched for almost three years thereafter until the incident occurred. The PDPC reiterated that it was necessary for organisations to conduct regular reviews and monitoring of their information and communication technologies systems, including software patches and updates.

© WongPartnership LLP
DISCLAIMER: This update is intended for your general information only. It is not intended to be nor should it be regarded as or relied upon as legal advice. You should consult a qualified legal professional before taking any action or omitting to take action in relation to matters discussed herein.
WongPartnership LLP (UEN: T08LL0003B) is a limited liability law partnership registered in Singapore under the Limited Liability Partnerships Act 2005.

Second, TCL SG did not implement processes to manage software patches and upgrades. In particular, software patching was done on an *ad hoc* basis by TCL SG's IT vendor on the instructions of TCL SG. However, because TCL SG was unaware of the patch, it did not instruct its IT vendor to install it. TCL SG's contract with the IT vendor also did not contain any requirements to conduct regular monitoring.

The PDPC observed that TCL SG could have, for example, implemented processes by which TCL SG or its IT vendors were automatically notified of available software patches or reminded to conduct checks for such patches. Further, the contract between TCL SG and its IT vendor could have specifically obliged the IT vendor to conduct such checks, without the need for TCL SG to provide instructions for patching on an *ad hoc* basis.

Third, TCL SG did not implement MFA for its administrator accounts despite these accounts having access to confidential and sensitive personal data. The PDPC reiterated that MFA is a baseline requirement for accounts with access to confidential or sensitive personal data or large volumes of personal data.

In the circumstances, the PDPC imposed a financial penalty of $82,000 on TCL SG. In coming to its decision, the PDPC noted that TCL had been cooperative, voluntarily accepted responsibility and conducted remedial actions. However, it also noted the Subject Data comprised a large volume of sensitive personal data, and the patch had been available for two years and nine months since TCL SG first started using the firewall device.

A copy of this decision may be accessed here.

© WongPartnership LLP
DISCLAIMER: This update is intended for your general information only. It is not intended to be nor should it be regarded as or relied upon as legal advice. You should consult a qualified legal professional before taking any action or omitting to take action in relation to matters discussed herein.
WongPartnership LLP (UEN: T08LL0003B) is a limited liability law partnership registered in Singapore under the Limited Liability Partnerships Act 2005.

Practical Guidance to Zuellig Pharma

Comments

In a practical guidance issued by the PDPC to Zuellig Pharma (**ZP**), the PDPC reiterated that express consent from individuals will not be required to transfer their personal data to a third-party intermediary.

The PDPC also provides useful insight into the considerations which should be taken into account when engaging a third-party intermediary and when using hashing techniques to protect personal data.

Background

ZP is implementing a privacy enhancing technology (**PET**) solution in its environment which third-party organisations (**TPOs**) are allowed to access and use.

A TPO can make use of the PET solution by transferring the relevant data into a secure region of ZP's environment (**Trust Execution Environment** or **TEE**). The TPO will then use a web application provided by ZP to apply a hashing algorithm to the fields of data which contain personal or sensitive data.

ZP sought guidance from the PDPC on whether the TPO's transfer of personal data (**Subject Data**) into ZP's TEE constitutes disclosure under the PDPA. If so, the TPO is required to obtain consent from the individuals to whom the personal data relate.

The PDPC's Assessment

The PDPC takes the view that the TPO would be engaging ZP as a data intermediary to provide hashing services through ZP's TEE and web application.

The PDPC reiterated that express consent from the individuals associated with personal data is not required for a firm to transfer such information to a third-party data intermediary organisation for processing. Since ZP will not use or access the Subject Data for other purposes, the TPO may transfer personal data into ZP's TEE without obtaining consent from the individuals concerned.

That being said, the PDPC highlighted the following points:

(a) The contract between the TPO and ZP should clearly specify the scope of work that ZP is to perform on the TPO's behalf and its purposes, as well as each party's responsibilities and liabilities in relation to the Subject Data;

(b) ZP, as a data intermediary of the TPO, should remain aware that it is subject to the Protection, Retention Limitation, and Data Breach Notification Obligations in respect of the Subject Data; and

(c) When using hashing techniques, proper safeguards should be implemented to prevent attackers from identifying individuals through inferences from pre-computed tables, and ZP and the TPO may wish to ensure that the hashes generated should be reasonably strong to protect the Subject Data. This is especially so for data that follows pre-determined formats or parameters such as NRIC numbers or race.

© WongPartnership LLP
DISCLAIMER: This update is intended for your general information only. It is not intended to be nor should it be regarded as or relied upon as legal advice. You should consult a qualified legal professional before taking any action or omitting to take action in relation to matters discussed herein.
WongPartnership LLP (UEN: T08LL0003B) is a limited liability law partnership registered in Singapore under the Limited Liability Partnerships Act 2005.

The PDPC also referred to other guidelines it has published which may be relevant to the use of hashing techniques to protect personal data. These include the Guide to Basic Anonymisation and Guide on Data Protection Blockchain Designs.

A copy of this practical guidance may be accessed here.

Practical Guidance to Meta

Comments

In this practical guidance, the PDPC provides useful insight into the key roles and responsibilities of various stakeholders for the purposes of data anonymisation and data processing. In particular, the PDPC sets out various considerations and safeguards to lower the risk of identification and re-identification of anonymised data.

Background

Meta is implementing a Proof of Concept (**POC**) on Interoperable Private Attribution (**IPA**) to measure the advertising impressions on conversions without the use of third-party cookies or mobile device identifiers. The IPA solution uses PETs like multiparty computing (**MPC**) and differential privacy (**DP**) to generate the attribution report.

The IPA solution architecture involves the following stakeholders:

(a) The organisation that owns or supplies digital advertising space (e.g., social media website, news publishing sites, software platforms) (**Publisher**);

(b) The organisation that buys digital advertising space for their marketing campaigns (e.g., brand owners) (**Advertiser**);

(c) The organisation that provides services to brands associated with creating, planning and managing advertising campaigns (**Adtech Entity**);

(d) The organisation that (i) develops or provides Internet browsing services, or (ii) develops or provides a mobile operation system for which developers create Internet-connected applications (**Platform Provider**); and

(e) The organisation that performs the MPC (**Helper Party**). The IPA architecture uses three Helper Parties for the MPC.

The following example illustrates how attribution reports are generated under the POC:

(a) An Advertiser runs an advertising campaign on a Publisher's website or app. For the purposes of attribution measurement, the Advertiser and Publisher will agree on the relevant activity data fields needed to measure the conversion value attributed to the Publisher for the advertising

© WongPartnership LLP
DISCLAIMER: This update is intended for your general information only. It is not intended to be nor should it be regarded as or relied upon as legal advice. You should consult a qualified legal professional before taking any action or omitting to take action in relation to matters discussed herein.
WongPartnership LLP (UEN: T08LL0003B) is a limited liability law partnership registered in Singapore under the Limited Liability Partnerships Act 2005.

campaign. The agreed activity data fields do not include any information that can directly identify an individual.

(b) A unique browser / device key will be generated by the Platform Provider for each user upon installation of the browser or mobile operating system, which will permanently reside with the user and will not be accessible by any party (including the Platform Provider). The browser / device key will be "shredded" and encrypted to generate a set of three encrypted secret share pairs (**ESSPs**). Each ESSP is encrypted such that each Helper Party can only decrypt its assigned ESSP.

(c) The Publisher and Advertiser will each extract the agreed activity data fields for attribution measurement and append the ESSPs before sharing them with an Adtech Entity for sorting and filtering purposes.

(d) The Adtech Entity will sort and filter the necessary activity data before "shredding" them into three random secret shares. Each pair of activity data secret shares will be shared with the corresponding ESSP to the respective Helper Party.

(e) Each Helper Party processes the activity data secret share to generate two "shreds" of the attribution report which is then shared with the Adtech Entity. The Adtech Entity merges the three unique "shreds" of the report to generate the desired attribution report. The attribution report is shared only with the Advertiser and Publisher.

Meta sought guidance from the PDPC on:

(a) Whether the data involved in the POC constitutes anonymised data such that the data protection provisions under the PDPA do not apply;

(b) The roles and responsibilities of the key stakeholders under the PDPA; and

(c) Additional safeguards and considerations to lower the risk of identification or re-identification.

PDPC's Assessment

The PDPC highlighted that it generally uses a risk-based approach in determining whether or not data is considered anonymised.

In the present case, the output from the PET implementation is considered to be anonymised data as long as the risk of reconstructing the browser / device key and activity data remains reasonably low. This risk would be assessed in view of any technical, governance and contractual safeguards implemented system-wide in the IPA implementation.

In light of the above, the PDPC provided some recommendations on some of the technical, governance and process safeguards that can be put in place by each stakeholder to lower the risk of re-identification, as further discussed below.

© WongPartnership LLP
DISCLAIMER: This update is intended for your general information only. It is not intended to be nor should it be regarded as or relied upon as legal advice. You should consult a qualified legal professional before taking any action or omitting to take action in relation to matters discussed herein.
WongPartnership LLP (UEN: T08LL0003B) is a limited liability law partnership registered in Singapore under the Limited Liability Partnerships Act 2005.

Publisher and Advertiser

Based on the details of the POC, the PDPC considered the Publisher and Advertiser to be data controllers that share activity data with the Adtech Entity for both the Publisher's and Advertiser's purposes.

As data controllers, the Publisher and Advertiser should assess and minimise any downstream risks of re-identifying any individual by other stakeholders or unauthorised parties from the activity shared and the generated attribution report. For example:

(a) The Publisher and Advertiser should apply the principle of data minimisation and only select activity data fields that are relevant to the generation of the agreed attribution report. Where possible, they should remove any direct or common identifiers, and consider using activity data fields that are less likely to identify any individual.

(b) In determining the structure and quantity of the attribution reports to be generated by the Adtech Entity, the Publisher and Advertiser should take reasonable measures to reduce the risk of individual linkage. Where the attribution report(s) can be used to reveal personal data about an individual to another stakeholder (i.e., Advertiser or Publisher), the PDPC highlighted that this will be considered a disclosure of personal data.

Adtech Entity

The PDPC considered the AdTech Entity to be a data intermediary that processes personal data on behalf of and for the purposes of both the Publisher and Advertiser.

Express consent is not required for an organisation to share personal data with its data intermediary to process personal data on its behalf. Therefore, consent is not required for the Adtech Entity to collect, sort, filter and "shred" the activity data for the purposes of generating the attribution report for the Publisher and Advertiser.

However, the PDPC highlighted that, as a data intermediary, the Adtech Entity will remain subject to the Protection, Retention Limitation and Data Breach Notification Obligations under the PDPA.

Further, if the Adtech Entity uses the activity data beyond what is required and agreed with the Publisher and Advertiser, then it would be considered a data controller. As a result, it would be subject to all the data protection obligations under the PDPA, including the need to obtain consent from the individual.

Platform Provider

With regard to the Platform Provider, the PDPC took the view that the Platform Provider will not be collecting personal data by generating the browser / device key, nor would it be using personal data by "shredding" and encrypting said browser / device key.

This is because the browser / device key is intended to be kept hidden from any parties and will not be combined with any data that the Platform Provider or any other third parties may have to identify the user.

© WongPartnership LLP
DISCLAIMER: This update is intended for your general information only. It is not intended to be nor should it be regarded as or relied upon as legal advice. You should consult a qualified legal professional before taking any action or omitting to take action in relation to matters discussed herein.
WongPartnership LLP (UEN: T08LL0003B) is a limited liability law partnership registered in Singapore under the Limited Liability Partnerships Act 2005.

Accordingly, the personal data protection obligations under the PDPA would not apply.

Helper Parties

Based on the activities undertaken by Helper Parties, the PDPC took the view that this group of stakeholders will not be subject to the PDPA because they would be processing anonymised data.

Other safeguards and considerations

The PDPC also highlighted the following considerations for the purposes of lowering the risk identification or re-identification of anonymised data.

(a) As the browser / device key is designed to be permanent and unique, there is a risk that it would be regarded as personal data because it has the characteristics of an identifier which could be used to combine other information about the user.

To mitigate this risk, additional safeguards that can be put in place include: deploying a temporary browser / device key (instead of a permanent one), ensuring that the browser / device key is generated and used solely for the attribution report, and ensuring that the "shredding" techniques used are sufficiently robust.

(b) There are also risks of re-identification of individuals due to the critical role the Helper Parties play in the IPA solution architecture.

To mitigate this risk, additional safeguards that can be put in place include: ensuring Helper Parties do not attempt to collude or re-identify any individual from the anonymised data through contractual means or other governance obligations, implementing technical safeguards to prevent or red-flag possible collusion between Helper Parties, and ensuring that Helper Parties put in place baseline measures to protect and secure their secret keys from compromise.

A copy of this practical guidance may be accessed here.

If you would like information or assistance on the above or any other area of law, you may wish to contact the Partner at WongPartnership whom you normally work with or any of the following Partners:

LAM Chung Nian
Head – Intellectual Property, Technology & Data
d: +65 6416 8271
e: chungnian.lam@wongpartnership.com
Click here to view Chung Nian's CV.

Kylie PEH
Partner – Intellectual Property, Technology & Data
d: +65 6416 8259
e: kylie.peh@wongpartnership.com
Click here to view Kylie's CV.

Connect with WongPartnership.

© WongPartnership LLP
DISCLAIMER: This update is intended for your general information only. It is not intended to be nor should it be regarded as or relied upon as legal advice. You should consult a qualified legal professional before taking any action or omitting to take action in relation to matters discussed herein.
WongPartnership LLP (UEN: T08LL0003B) is a limited liability law partnership registered in Singapore under the Limited Liability Partnerships Act 2005.

WPG MEMBERS AND OFFICES

- contactus@wongpartnership.com

SINGAPORE

-
WongPartnership LLP
12 Marina Boulevard Level 28
Marina Bay Financial Centre Tower 3
Singapore 018982
t +65 6416 8000
f +65 6532 5711/5722

CHINA

-
WongPartnership LLP
Shanghai Representative Office
Unit 1015 Link Square 1
222 Hubin Road
Shanghai 200021, PRC
t +86 21 6340 3131
f +86 21 6340 3315

INDONESIA

-
Makes & Partners Law Firm
Menara Batavia, 7th Floor
Jl. KH. Mas Mansyur Kav. 126
Jakarta 10220, Indonesia
t +62 21 574 7181
f +62 21 574 7180
w makeslaw.com

MALAYSIA

-
Foong & Partners
Advocates & Solicitors
13-1, Menara 1MK, Kompleks 1 Mont' Kiara
No 1 Jalan Kiara, Mont' Kiara
50480 Kuala Lumpur, Malaysia
t +60 3 6419 0822
f +60 3 6419 0823
w foongpartners.com

MIDDLE EAST

-
Al Aidarous Advocates and Legal Consultants
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
t +971 2 6439 222
f +971 2 6349 229
w aidarous.com

-
Al Aidarous Advocates and Legal Consultants
Oberoi Centre, 13th Floor, Marasi Drive, Business Bay
P.O. Box No. 33299
Dubai, UAE
t +971 4 2828 000
f +971 4 2828 011

PHILIPPINES

-
Gruba Law
27/F 88 Corporate Center
141 Valero St., Salcedo Village
Makati City 1227, Philippines
t +63 2 889 6060
f +63 2 889 6066
w grubalaw.com

wongpartnership.com