Changes to the Data Protection Regulatory Landscape

The Singapore Personal Data Protection Commission has announced major updates to the data protection framework in Singapore

Overview

The Singapore Personal Data Protection Commission ("**PDPC**") has recently introduced various updates to the data protection regime in Singapore by releasing new guidelines to enhance accountability in the handling of personal data and also public consultations on data portability and data innovation.

(i) Strengthening data protection measures and fostering greater accountability

Following certain high profile data protection incidents, the PDPC has sought to strengthen data protection management and accountability across organisations. The revised measures are significant in signifying a fundamental shift in focus from mere compliance to prescriptive rules, to a broader context of the design and implementation of underlying frameworks and systems for data management, coupled with increased emphasis on accountability within each organisation's corporate governance structure.

In particular, directors and senior management are expected to play greater roles in the implementation and management of processes, systems and measures in the handling and management of data:

(a) A new **Guide to Data Protection by Design for ICT Systems** was issued to provide guidance on the application of "Data Protection by Design" principles in the design and development of information and communications technology ("**ICT**") systems.

It is hoped that by considering data protection principles at the onset, ICT systems can be designed from the ground up to specifically address and entrench such principles so that organisations can build robust data protection management frameworks in meeting their regulatory requirements.

(b) Amendments to the **Guide to Developing a Data Protection Management Programme** were effected to enhance the role and responsibilities of senior management and directors in the oversight of the organisation's data policies, processes, systems and risk management, for compliance with data regulations.

(ii) Data breach incidents and changes to the enforcement regime

(a) As a precursor to the upcoming legislative implementation of the mandatory data breach notification regime in the Personal Data Protection Act ("**PDPA**"), the **Guide to Managing Data Breaches 2.0** was released to provide further compliance guidance to organisations on data breach management and reporting.

© 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 (Chapter 163A).

Under this updated guide:

(i) organisations are encouraged to put in place monitoring measures for early detection of data breaches, and a data management plan for steps to be taken in assessing and reporting of a data breach; and

(ii) The PDPC expects to be notified of data breach incidents where 500 or more individuals are affected, or where significant harm or impact to the individual is likely to result; and no later than 72 hours from the time those organisations complete their investigations and assessments of a potential data breach, and not beyond 30 days of discovery of the incident.

(b) A new **Guide on Active Enforcement** was issued, which sets out the PDPC's approach to dealing with enforcement matters. In particular, two new processes were introduced:

(i) a **new expedited decision process** which aims to conclude investigations on clear-cut data breaches more expeditiously. An organisation's upfront admission of liability for breaching the PDPA, and the similarity of the facts of the data breach to other precedent cases are factors which the PDPC will take into consideration in determining if the matter qualifies for the new expedited decision process; and

(ii) an **undertaking option**, whereby organisations may request to undertake to execute a contingency plan as a resolution for a data breach that has occurred. To be considered for this option, organisations need to demonstrate that they have in place the proper framework for accountability, monitoring and remediation.

(iii) Proposed introduction of data portability and data innovation frameworks

To support innovation in a digital economy, for which data plays an increasingly central role, the PDPC also launched a **Consultation on Proposed Data Portability and Data Innovation Provisions** to seek feedback and views on the introduction of the following concepts into the PDPA regime:

(a) **Data portability** – to facilitate data flow and sharing, the PDPC is considering conferring rights on individuals to request for the movement of their data across organisations and empower consumers with enhanced choice and control over the use of their data; and

(b) **Data innovation** – in recognising the importance of the use of data analytics for the development of new and improved products, the PDPC is considering facilitating and enabling secondary uses of data by organisations for which consent from data subjects need not be sought, and which will also be exempt from certain obligations under the PDPA. In this connection, the new concepts of "**derived data**" and "**business innovation purposes**" are being considered.

We elaborate below on the salient highlights and issues to take away from these updates and initiatives.

© 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 (Chapter 163A).

(A) Enhanced regulatory framework: strengthening data protection measures and fostering greater accountability

(i) Protection by Design for ICT systems

Data protection by design ("**DPbD**") establishes the concept that pre-emptive, and not merely reactive data protection measures should be adopted in relation to personal data processed when designing and implementing IT systems, business practices and network infrastructure.

The new Guide to Data Protection by Design for ICT systems ("**DPbD ICT Guide**") serves to set out guidelines and encourage organisations in applying DPbD principles in the context of design and development of ICT systems, as part of establishing a robust data protection management framework for the organisation's regulatory compliance.

The DPbD ICT Guide advocates that consideration of data protection principles at the outset enables the creation and embedding of a good data management culture that can be carried through the entire lifecycle of the ICT system, rather than being addressed on a piecemeal basis or retrofitted as an afterthought. In particular, a data protection impact assessment ("**DPIA**") is recommended to be performed at the outset, regardless of whether the "waterfall" software development model or agile software development approach is used.

To elaborate further, the DPbD ICT Guide outlines and identifies key DPbD principles which are relevant to, and can be potentially embodied in, the ICT context:

- **Proactive and preventive:** To manage and minimise risks through good design and data management practices.
- **Data protection as the default:** To integrate data protection measures into processes and features of the systems. Measures to safeguard personal data should be automatically provided as default settings and individuals should not have to take active action for protection.
- **End-to-end security:** Good security features and practices should be incorporated end-to-end at every stage of the software development life cycle. Users should consider how their organisations and vendors, as well as how the components of the ICT system, work together.
- **Data minimisation:** Collect, store and use personal data that is strictly relevant and necessary for the intended purposes for which data is processed.
- **User-centric:** ICT systems should be developed with individuals in mind, with the goal of protecting their personal data. This can be effected through default settings whilst giving individuals flexibility in customising settings. Such interfaces should also be user-friendly.
- **Transparency:** Taking an active role in notifying individuals on what personal data is collected and how it should be used, and identifying and using the most appropriate means to provide such information.

© 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 (Chapter 163A).

- **Risk minimisation**: Systematically identify and mitigate risks by designing and implementing appropriate processes and relevant ICT security measures when processing personal data.

Additionally, the DPbD ICT Guide provides helpful guidance in presenting a list of more than 60 good practice tips that users may adopt and adapt accordingly as may be appropriate for their ICT projects. The topics range from DPIA, development of the ICT system, collection of personal data by ICT systems, getting consent for users' personal data, to user device security and the maintenance phase.

(ii) Enhanced role of senior management and directors in data protection management

In tandem, revisions to the Guide to Developing a Data Protection Management Programme ("**DPMP Guide**") seek to reinforce data protection accountability within the organisational structure.

The DPMP Guide provides guidance and benchmarking standards for the implementation of a Data Protection Management Programme that is tailored to an organisation's specific needs.

It is noteworthy that the DPMP Guide articulates senior management's obligations in data protection and management as part of their overall corporate governance risk management responsibilities. For example:

- the monitoring and managing of personal data protection risks and, where relevant, reporting the same to the Board of Directors, is explicitly identified as a role for senior management; and

- in relation to the recommendation to implement mechanisms and processes for regular reporting of data protection risks and remedial measures to senior management, the DPMP Guide makes reference to the Board Risk Committee Guide as a source of guidance for the Board of Directors' general oversight role in ensuring the adequacy and effectiveness of the organisation's risk management and internal controls.

These amendments are clear signals that the board of directors and the senior management are now expected to play an enhanced role in ensuring compliance with the PDPA, and will be held to greater accountability.

(iii) Data Protection Trustmark ("DPTM") Certification as external validation process

In encouraging organisations to obtain an objective assessment and external validation of the robustness of their data protection practices and processes, the DPMP Guide additionally recommends that organisations consider validating and certifying their Data Protection Management Programme through the DPTM Certification.

The DPTM Certification, newly launched in January 2019, is a voluntary enterprise-wide certification to assist organisations to demonstrate accountable and responsible data protection practices, and building trust and confidence in customers.

© 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 (Chapter 163A).

Notably, the PDPC has also suggested that whether an organisation is DPTM certified is a relevant factor that it will consider when determining if it will accept that organisation's undertaking in discharging its enforcement action against that organisation's data breach(es)[1].

(B) Managing and enforcing data breaches

(i) Data breach management - preparing for the introduction of mandatory breach notification regime

In relation to managing data breach incidents, updates to the Guide to Managing Data Breaches ("**Data Breach Guide**") serve to provide an organised framework and further granularity as to the practical steps which an organisation should undertake in data breach incidents.

In this regard, the updates to the Data Breach Guide primarily focus on the aspects of (i) pre-emptive measures to be taken in preparing for data breaches; and (ii) reporting and notification obligations upon occurrence of the breach.

In terms of pre-emptive measures, the Data Breach Guide repeats the need to put in place a robust data management plan for organisations to respond to data breaches more expeditiously. Whilst the plan has to be tailored to each organisation's bespoke business processes and needs, the PDPC recommends that the plan sets out the following high-level framework:

- A clear explanation of what constitutes a data breach;
- How to report a data breach internally;
- How to respond to a data breach; and
- Responsibilities of the data breach management team.

In terms of responding to data breaches, the overall thrust remains largely the same – i.e., the PDPC recommends that actions taken after a data breach should follow four key steps under the "C.A.R.E." framework. In this latest round of amendments however, organisations should especially take note of the updated reporting and notification obligations, which should follow the refreshed "points of notifications" guidelines issued by the PDPC.

A summary of the salient details of the guidelines on notification is set out below.

Time frame for assessing a data breach	• Within 30 days upon becoming first aware of a potential data breach.

[1] *Please refer to the section above on the Guide of Active Enforcement for further details on enforcement actions.*

© 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 (Chapter 163A).

When is notification necessary?	• When the breach: (a) is likely to result in significant harm or impact to the individuals to whom the information relates; or (b) is of a significant scale (i.e., the data breach involves personal data of **500 or more individuals**).
Who should be notified?	• The PDPC. • Affected individuals, when the breach is likely to result in significant harm or impact to such individuals.
What is the timeline for notification?	• As soon as practicable, and to the PDPC, **not later than 72 hours**.
What form should the notification take?	• To the PDPC: by way of email or call. • To affected individuals: organisations are required to work with the PDPC to determine if notification is required. If so, organisations need to consider the most effective way to reach individuals, taking into consideration the urgency of the situation, and the number of individuals affected.
Details to be included in the notification	• Notifications to the PDPC and affected individuals must specify certain stipulated details.

(ii) Introduction of an Active Enforcement Framework

On the enforcement end, the PDPC, in recognising the need to efficiently handle and manage the volume of complaints and incidents filed, has now organised its deployment of enforcement powers into an Active Enforcement Framework ("**Framework**"), setting out a tiered approach which is calibrated to the extent and severity of breach in question.

Of particular interest is the introduction of the **undertaking option** and the **expedited breach decision process**, both of which enable the expeditious conclusion of a data breach case:

- The **undertaking option** enables organisations to provide a written agreement to the PDPC on the steps it commits to remedy the breach and prevent further occurrences, and is no doubt helpful to organisations in concluding the matter and preferable to being subject to financial penalties or other sanctions.
- The **expedited breach decision process**, on the other hand, allows the PDPC to more quickly conclude the case and issue a decision, to reduce or eliminate time spent on investigations, which could be likewise costly and disruptive on the organisation's part.

© 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 (Chapter 163A).

A summary of the types of enforcement actions under the Framework is set out below.

Suspension or discontinuation of investigation	• Generally considered where the impact is assessed to be low. • In such scenarios, an advisory notice will be issued, highlighting areas of improvement.
Undertaking	• Written agreement between organisation and the PDPC where an organisation commits to remedy and take steps to prevent recurrence of such breaches. • Organisation *must request to invoke process as soon as possible after the incident is known*, i.e., upon commencement or in the early stages of investigations. Additional time will not be given to produce the remediation plan. • Acceptance of undertaking is at the PDPC's sole discretion. A key consideration is the effectiveness of the remediation plan and the organisation's readiness to implement it forthwith. In particular, the PDPC may be prepared to accept undertaking where: o the organisation has accountable practices in place (e.g., a Data Protection Trustmark certified organisation) and is ready to implement its remediation plan; or o the PDPC is of the view that undertaking achieves a similar or better enforcement outcome more effectively and efficiently than a full investigation.
Expedited Decision	• The PDPC may at its discretion consider an expedited decision where there is an upfront admission of liability. • To be considered, organisations must make a written request to the PDPC when investigations commence. Organisations must also be prepared to admit liability. This will also be a strong mitigating factor in determining financial penalties (unless in cases of repeated data breaches). • Generally, the PDPC will consider having an expedited decision in the situations when: o the only breach of the PDPA is that the organisation has no Data Protection Officer and/or no Privacy Policy; or

© 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 (Chapter 163A).

	o the nature of the data breach is similar to precedent cases with similar categories of facts, e.g., poor password policy, or occurrence of printing or enveloping errors.
Full Investigation Process	• Usually involves high impact incidents, such as where a large number of individuals was affected and the personal data disclosed could cause significant harm. • The full investigation process may result in the following decisions: no breach, warning, directions, financial penalties, or directions and financial penalties.

Additionally, the Guide on Active Enforcement also sets out various guiding factors in relation to the determination of financial penalties. Generally, financial penalties are reserved only for breaches which are particularly serious in nature.

In assessing the seriousness of the breach and the amount of financial penalties to be levied, various considerations will be taken into account by the PDPC, including:

- impact of the breach;
- whether the organisation had, or ought to have, known the risk of a serious contravention and failed to take reasonable preventive steps;
- number of individuals whose personal data had been subjected to harm and risks;
- types of personal data that were put at risk;
- cooperativeness of the organisation during investigations;
- whether remedial action(s) were implemented;
- whether there was voluntary notification of the data breach;
- whether the organisation had engaged with the affected individuals in a meaningful manner and had voluntarily offered a remedy, and that the individuals had accepted the remedy; and
- whether the organisation admitted to liability for the data breach.

(C) Proposed introduction of data portability and data innovation provisions

Building on an earlier data portability discussion paper issued in February 2019, this round of public consultation seeks feedback and views to provide a balanced regulatory approach in support of the fostering of a digital economy, by introducing provisions relating to two key concepts: **(1) data portability** and **(2) data innovation**.

© 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 (Chapter 163A).

Whilst the proposed amendments are still at the consultation stage, and may be subject to further changes, once implemented, the data portability and data innovation provisions would have significant knock-on effects, and businesses will need to adapt their systems and re-examine (or re-negotiate) their existing contracts with service providers and data intermediaries.

Organisations should therefore watch this space closely for upcoming changes, so as to plan ahead as early as possible to devise appropriate internal policies and measures for compliance.

The proposed key features are as follows:

(i) Data Portability Obligation

Under the proposed data portability obligation, an organisation must, at the individual's request, provide the individual's data that is in the organisation's possession or under its control to another organisation in a commonly used machine-readable format ("**Data Portability Obligation**").

The following have been proposed as regards the Data Portability Obligation:

(a) **Applicability to Organisations:** The Data Portability Obligation will apply to any organisation that collects, uses or discloses personal data in Singapore, except for organisations falling outside of the scope of the PDPA and data intermediaries.

(b) **Scope of Transmission:** Organisations will only be required to transmit data to other organisations that have a presence in Singapore (i.e., formed or recognised under the law of Singapore; and resident, or having an office or place of business in Singapore).

(c) **Scope of Data:** Subject to exceptions, the Data Portability Obligation will apply to data that is: (i) provided by the individual to the organisation ("**user provided data**"); and/or (ii) generated by the individual's activities in using the organisation's product or service ("**user activity data**"), to the extent that the data is in the possession or control of the organisation and is held in electronic form.

Notably, user provided data and user activity data are potentially broader than personal data (as defined under the PDPA), and may further include the individual's business contact information, as well as personal data of third parties (insofar as provided by the requesting individual or generated by the individual's activities).

(d) **Exceptions:** The PDPC has proposed for the Data Portability Obligation to be subject to similar exceptions to the access obligation under section 21 of the PDPA. Notably, it is proposed that the exceptions include the new proposed category of "derived data" (as elaborated further below).

(e) **Handling of Requests:** Several obligations of the porting organisation in handling a data porting request have been proposed, including:

- providing an avenue for individuals to submit data porting requests;

© 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 (Chapter 163A).

- ensuring the veracity of the data portability request and allowing the requesting individual to review the data (or a sample of the data) before transmission to the receiving organisation;
- providing information on reasonable fees payable and time frame for porting; and
- adopting an easily accessible and affordable format for porting data to facilitate interoperability, and providing technical information about the data formats used and the relevant protocols for transmission and receipt.

(f) **Responsibilities of Receiving Organisations:** The receiving organisation will have the right to not accept the data or to retain only a portion of the data if the data is irrelevant or excessive in relation to the product or service it provides. Correspondingly, key obligations of the receiving organisation in handling a data porting transmission have also been proposed, including:

- verifying the completeness and conformity to formats and standards of data transmitted to it; and
- obtaining consent and notifying individuals for the purposes for which the ported personal data accepted by the receiving organisation is collected, used and/or disclosed, because accepting ported personal data constitutes a collection of personal data subject to the PDPA and any other applicable laws.

(ii) Data Innovation Provisions

To foster data innovation, such as through the employment of data analytics, the PDPC also proposes to introduce the following concepts under the PDPA:

(a) A new category of data, "**Derived Data**", which refers to new data that is created through the processing of other data by applying business-specific logic or rules, will be introduced.

The PDPC proposes that derived personal data (i.e., derived data which constitutes personal data within the meaning of the PDPA) shall not be subject to the following obligations under the PDPA:

- access and correction obligations; and
- the proposed Data Portability Obligation.

However, organisations would still be required to comply with all other provisions of the PDPA applicable to personal data. For example, pursuant to the accuracy obligation, organisations would be required to make a reasonable effort to ensure that the derived personal data is accurate and complete if it is likely to make a decision that affects the individual, or to be disclosed to another organisation.

(b) The concept of **"Business Innovation Purposes"** to clarify that organisations can use personal data for the purposes of: (i) operational efficiency and service improvements; (ii) product and

© 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 (Chapter 163A).

service developments; or (iii) knowing customers better, without the requirement to notify the individuals of, and seek consent to, use their personal data for such purposes.

Furthermore, it is proposed that business innovation purposes will be considered business purposes for which retention of the personal data may be necessary.

However, unless an exception under the PDPA applies, organisations are still required to obtain the requisite consent and notification for the collection or disclosure of personal data, regardless whether for business innovation purposes or otherwise.

Concluding Remarks and Looking Ahead

The new initiatives introduced by the PDPC are far-reaching, and organisations will need to review their existing processes to ensure that they are updated to be aligned with the best practices and recommendations contained in the revised guidelines.

Organisations should also monitor developments on the introduction of regulatory requirements in relation to data portability as these can have far-reaching impacts on businesses, as well as introduce significant compliance costs. At the same time, the PDPC's proposals on data analytics is also very timely, and organisations should also pay close attention to whether the proposals are sufficiently flexible or whether more latitude is required.

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 work with or any of the following partners:

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

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

© 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 (Chapter 163A).

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
Beijing Representative Office
Unit 3111 China World Office 2
1 Jianguomenwai Avenue, Chaoyang District
Beijing 100004, PRC
t +86 10 6505 6900
f +86 10 6505 2562

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

MYANMAR

-
WongPartnership Myanmar Ltd.
Junction City Tower, #09-03
Bogyoke Aung San Road
Pabedan Township, Yangon
Myanmar
t +95 1 925 3737
f +95 1 925 3742

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 International Legal Practice
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 International Legal Practice
Zalfa Building, Suite 101 - 102
Sh. Rashid Road
Garhoud
P.O. Box No. 33299
Dubai, UAE
t +971 4 2828 000
f +971 4 2828 011

PHILIPPINES

-
ZGLaw
27/F 88 Corporate Center
141 Sedeño Street, Salcedo Village
Makati City 1227, Philippines
t +63 2 889 6060
f +63 2 889 6066
w zglaw.com/~zglaw

wongpartnership.com