

Kingdom of Saudi Arabia Personal Data Protection Law Series

Part 1 - Summary of the Personal Data Protection Law



Introduction

This “Kingdom of Saudi Arabia Personal Data Protection Law Series” addresses the following three aspects:

1

Part 1: A summary of the Personal Data Protection Law (“PDPL”)

2

Part 2: A summary of the Implementing Regulation of the PDPL (“**Implementing Regulation**”)

3

Part 3: A step-by-step guide to personal data transfers outside of the Kingdom of Saudi Arabia, based on the Regulation on Personal Data Transfer outside the Kingdom (“**Data Transfer Regulation**”)¹

On 14 September 2023, the PDPL came into force in the Kingdom of Saudi Arabia (“**KSA**”). The PDPL is the main law in KSA regulating the use of personal data. From 14 September 2023, entities have **one year to achieve compliance** with the PDPL and Regulations, which will all become fully enforceable from 14 September 2024.

All public and private entities must comply with the PDPL and Regulations.

The Saudi Authority for Data and Artificial Intelligence (“SDAIA”) is the Competent Authority that shall supervise the implementation of the PDPL and Regulations. The Competent Authority may request documents or information from entities to check their compliance.

The PDPL provides **finest (up to SAR 5,000,000) for breach** of its provisions and provisions of Regulations. The competent court may double the amount of the fine for data breaches in case of repetitive violations. The PDPL also provides for imprisonment (up to two years) for disclosure or publication of sensitive data (done in violation of the PDPL) with the intention to harm an individual or to achieve personal gain.



In this part 1 of our series, we look at the core concepts of the PDPL and what these will mean for the entities doing business in the KSA.

¹ In our series we refer jointly to Implementing Regulation and to Data Transfer Regulation as “Regulations”.

Scope of the Personal Data Protection Law (“PDPL”)

A. What does the PDPL regulate?



The PDPL regulates processing² of personal data. The scope of the PDPL includes:

processing of personal data of **any type** (e.g., contact information, health data, credit data, etc.)

01

processing of personal data from **any source** (e.g., provided by individuals directly to the entity or obtained by the entity from other sources, etc.)

02

processing of personal data in **any form** (e.g., electronic or paper, structured or unstructured, etc.)

03

Personal Data

The personal data is defined in the PDPL as follows³: any data, regardless of its source or form, that may lead to identifying an individual specifically, or that may directly or indirectly make it possible to identify an individual, including name, personal identification number, addresses, contact numbers, licence numbers, records, personal assets, bank and credit card numbers, photos and videos of an individual, and any other data of personal nature.

Therefore, any data based on which it is possible to identify an individual shall be considered as personal data under the PDPL.

Examples:

an individual's name



telephone number



bank account number



If it is impossible to identify a particular individual from the data in question, then such data is not personal data and its use is **not regulated by the PDPL**. For instance, anonymised data, sales figures, data about the number of overall visits on a web page.

Sensitive Data

The PDPL provides for a separate subset of personal data – “sensitive data”. It includes personal data revealing racial or ethnic origin, or religious, intellectual or political belief, security data, data relating to criminal offenses, biometric or genetic data, health data, and data that indicates that one or both of the individual's parents are unknown.

The PDPL provides for additional requirements and restrictions to processing sensitive data. For example:

- it is not allowed to rely on a lawful basis of “legitimate interest” when processing sensitive data⁴;
- it is forbidden to use sensitive data for marketing purposes⁵.



Please note that unlike many other data protection laws, the PDPL also regulates processing of data of deceased persons if such data allows the identification of the deceased person or their family members.

² “Processing” means any kind of use of personal data.

³ Article 1 (4) of the PDPL.

⁴ Art. 6 (4) of the PDPL.

⁵ Art. 26 of the PDPL.

B. Where does the PDPL apply?



The PDPL applies to the following processing of personal data by any means (manual or automated):

In the KSA

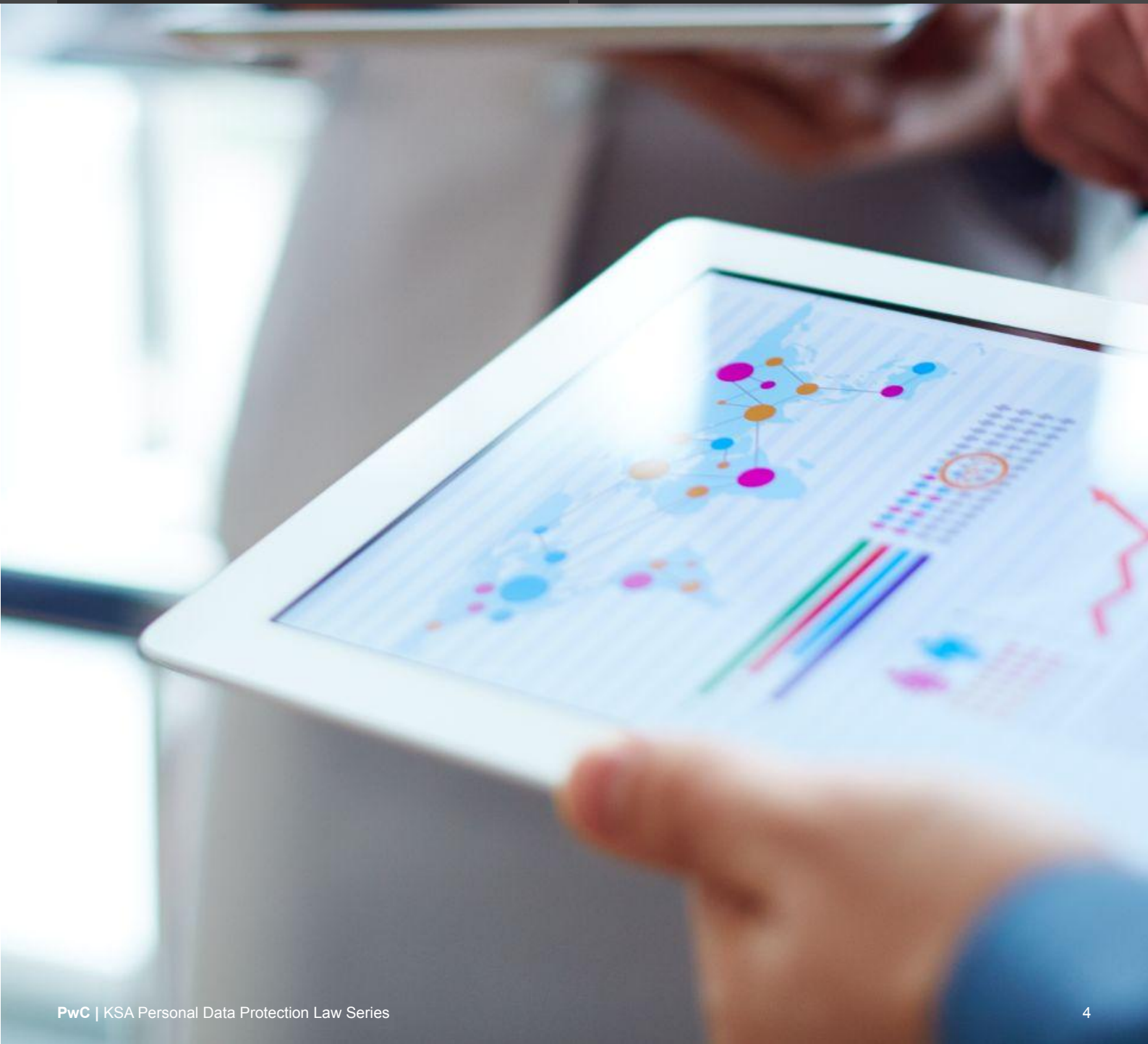
Any processing of personal data that takes place **in the KSA**, which means that the PDPL applies to processing of personal data on all territory on which the Kingdom has its authority, including the geographical territory of the Kingdom and its embassies in foreign jurisdictions

01

Outside the KSA

The processing of KSA residents' personal data **outside the KSA**, which means that the PDPL has extraterritorial application in relation to KSA residents (this may include Saudi citizens and other individuals who stay in the KSA permanently or temporary)

02



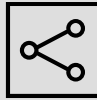
Roles and obligations of an entity under the PDPL

A. What are the roles that an entity can assume under the PDPL?



The PDPL provides for two roles for an entity in respect of the processing of personal data – a Controller and a Processor.

A Controller is an entity that makes decisions about the purposes and ways of the processing of personal data. The Controller is ultimately responsible for the processing under the PDPL.



A Processor is an entity that processes personal data on behalf of a Controller. As opposed to the Controller, the Processor does not make decisions about the purposes and ways of personal data processing and instead takes direction from the Controller.



B. What are the key obligations of a Controller?



- To define the purpose of the processing of personal data.
- To ensure that there is a suitable lawful basis for the processing of personal data (e.g., consent, legal obligation, legitimate interest, etc.).
- To ensure that personal data is processed pursuant to the principles of personal data processing (for example storage limitation, see further [Principles of personal data processing](#)).
- To notify data subjects⁶ on how their personal data is processed (for example, via a privacy notice).
- To enable data subjects to exercise their rights under the PDPL.
- To maintain records of processing activities register (“**RoPA**”) for all processing of personal data across the entity.
- To conduct impact assessments of personal data processing (for example, Data Protection Impact Assessment; Data Transfer Impact Assessment or Legitimate Interest Assessment).
- To ensure lawful cross-border transfers of personal data outside the KSA.
- To implement all the necessary organisational, administrative and technical measures to protect personal data.
- To cooperate only with those Processors that provide necessary guarantees to implement the provisions of the PDPL and the Regulations, to enter into data processing agreements with Processors, and to monitor compliance of Processors with such agreements.
- To notify any changes in personal data to entities to which the personal data was transferred.
- To notify the Competent Authority and data subjects of personal data breaches.
- To appoint a Data Protection Officer, where required by the Implementing Regulation⁷.
- To comply with requirements of the PDPL and Implementing Regulation to specific types of processing activities, for example:
 - processing of health data and credit data;
 - processing of personal data for sending advertising or awareness-raising materials;
 - processing of personal data for scientific, research, or statistical purposes;
 - disclosure of personal data;
 - copying official documents where data subjects are identifiable.
- To comply with the rules for registration of Controllers in the National Register of Controllers (the rules are to be issued by the Competent Authority).

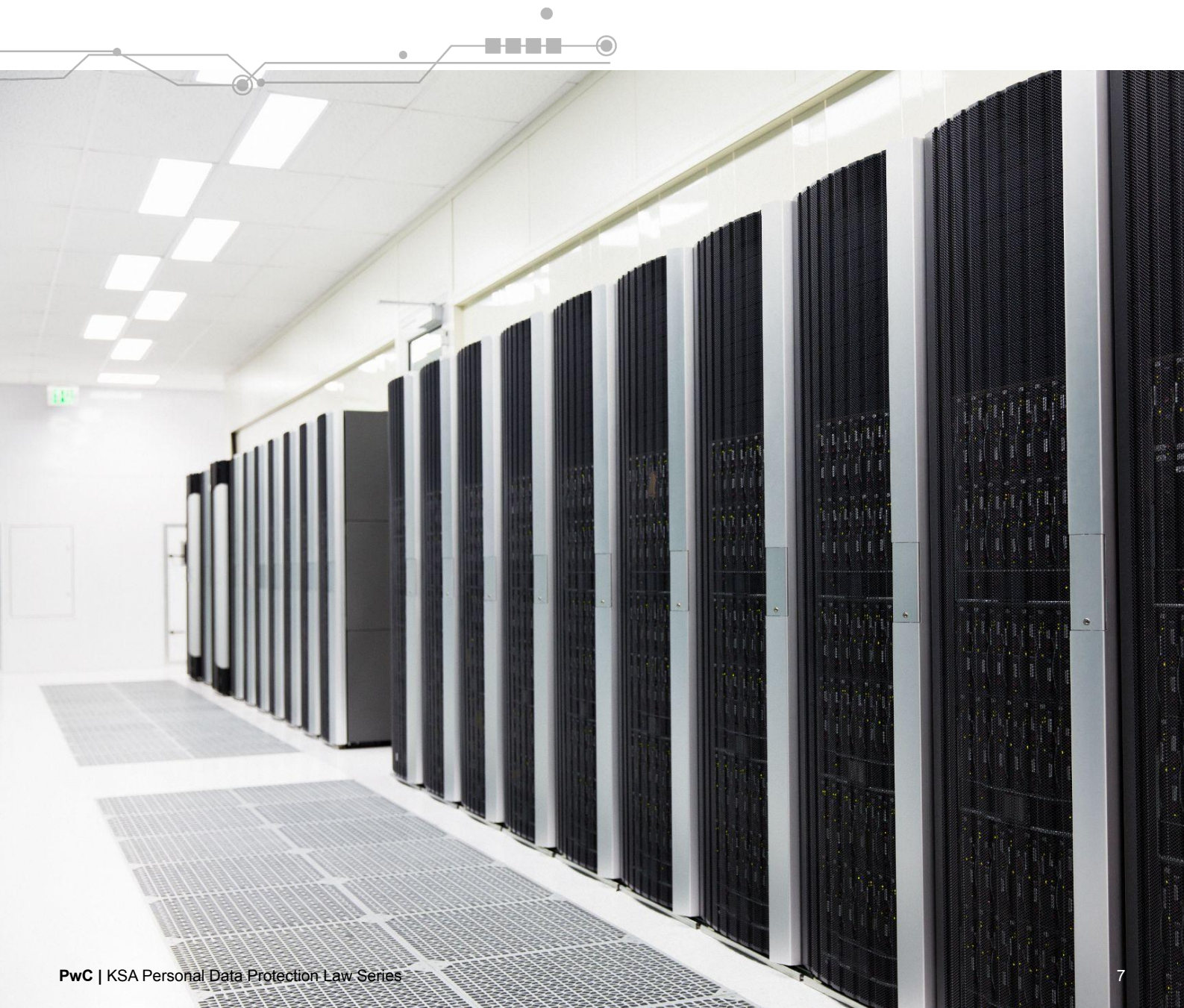
⁶ Data subjects are individuals whose personal data is processed.

⁷ Art. 30 (2) of the PDPL.

C. What are the key obligations of a Processor?










- To process personal data for the Controller based on a data processing agreement.
- To comply with instructions of the Controller regarding the personal data processing.
- To assist the Controller by implementing appropriate organisational, administrative and technical measures to protect personal data that it is processing for the Controller.
- Before a Processor engages with any sub-processor for the processing, to ensure the following:
 - the contracts with sub-processors will not impact the level of protection provided to the personal data being processed;
 - the sub-processors will provide sufficient guarantees to comply with the PDPL and the Regulations; and
 - the Processor shall notify the Controller on engaging a sub-processor and the Controller shall have the right to object to such engagement within a timeframe agreed upon between the Controller and the Processor.



Principles of personal data processing

Although the PDPL does not explicitly list any data protection principles, such principles are embedded in the PDPL's provisions. Understanding these principles helps to understand many of the requirements of the PDPL.

Principle	Description of the principle
 Lawfulness, fairness and transparency	Entity must: <ul style="list-style-type: none">ensure that it processes and discloses personal data only after having an appropriate lawful basis for such processing;process personal data only in ways that data subject would reasonably expect;be open and clear towards data subjects when processing personal data.
 Purpose limitation	Entity must: <ul style="list-style-type: none">have a specific purpose for processing the personal data, which must be documented in the RoPA;only collect and process personal data to fulfill a legitimate purpose, which is specified in the RoPA, and not process personal data beyond such a purpose.
 Data minimisation	Entity must only collect and process the minimum amount of personal data that is relevant, necessary, and adequate to fulfill the purposes for which it is processed.
 Storage limitation	Entity must process personal data no longer than is necessary for the purposes for which the personal data has been collected, unless processing (storing) for a longer time is required by the applicable laws.
 Accuracy	Entity must: <ul style="list-style-type: none">take reasonable measures to ensure that personal data is accurate and up to date (for example: it regularly reviews the personal data that it holds);provide an opportunity to individuals to correct and update their personal data, where necessary.
 Integrity and confidentiality	Entity must have in place appropriate technical and organisational measures to ensure security of personal data. Such measures shall protect the confidentiality, integrity and availability of personal data.
 Accountability	Entity must have appropriate measures and records in place to be able to demonstrate compliance with the PDPL.

Lawful bases for personal data processing

The Controller must ensure that it processes personal data only if having an appropriate lawful basis (ground) for such processing. The PDPL provides for several sets of lawful bases that should be used depending on particular circumstances of processing.

General lawful bases (Art. 5 and Art. 6 of the PDPL)

- **Consent** – data subject has given consent to the processing of his or her personal data.
- **Actual interests** – processing serves actual interests of the data subject, but communicating with the data subject is impossible or difficult.
- **Contract** – processing is pursuant to the implementation of a previous agreement to which the data subject is a party.
- **Legal obligation** – processing is required and regulated by another law.
- **Public interest** – if the Controller is a public entity and the processing is required for security purposes or to satisfy judicial requirements.
- **Legitimate interest** – processing is necessary for the purpose of legitimate interest of the Controller, provided that no sensitive data is to be processed.

Lawful bases for (i) collection of personal data from a source other than the data subject and for (ii) processing personal data for purposes other than the ones for which the personal data was initially collected (Art. 10 of the PDPL)

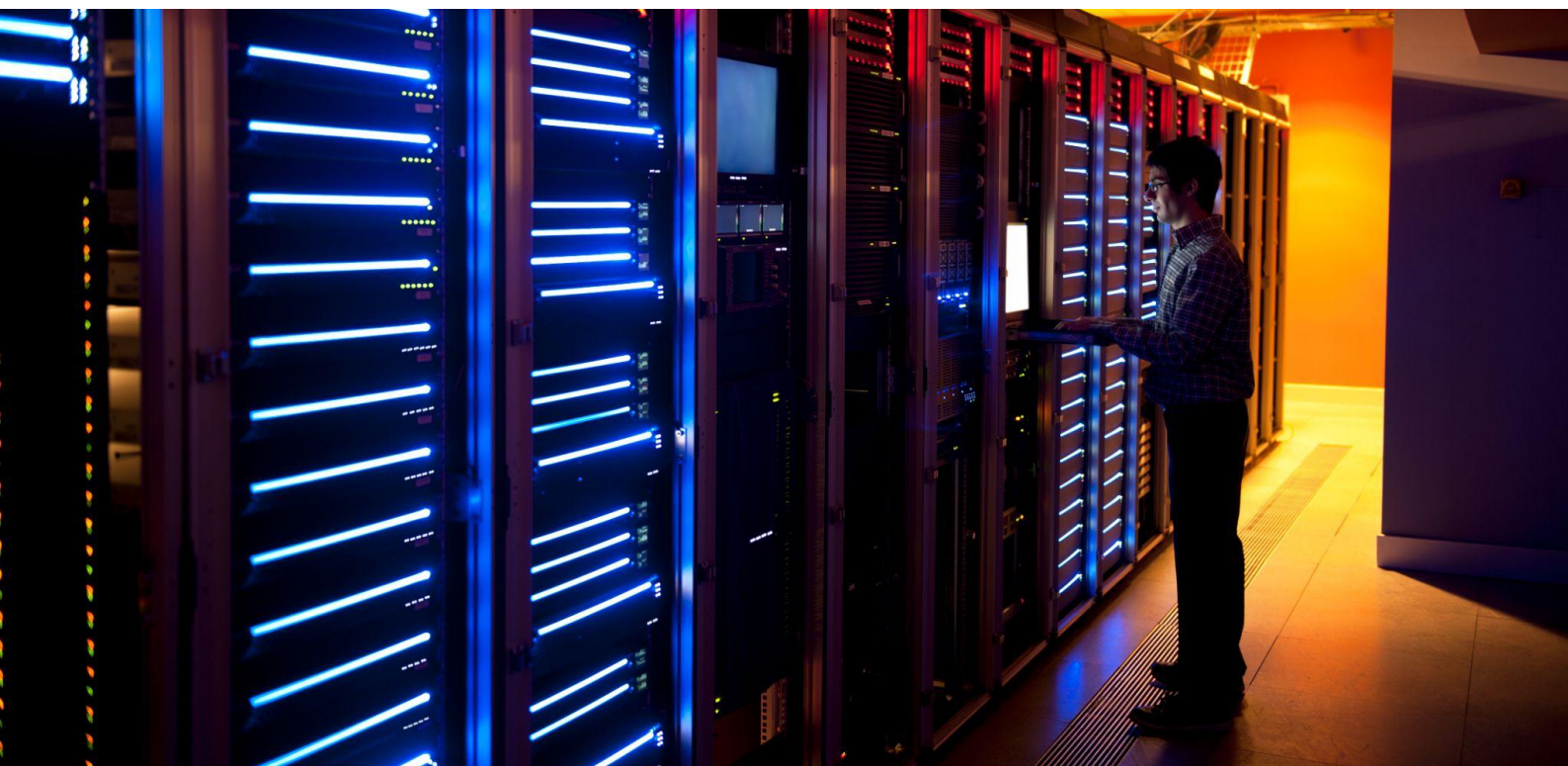
- **Consent** – data subject has given consent to the processing of his or her personal data.
- **Publicly available data** – personal data is publicly available or collected from a publicly available source.
- **Public interest or security purposes** – the Controller is a public entity and processing of personal data is required for public interest or security purposes, or to implement another law, or to fulfill judicial requirements.
- **Vital interests** – if not collecting or processing of personal data may harm the data subject or affect their vital interests.
- **Public health and safety** – personal data collection or processing is necessary to protect public health, public safety, or to protect the life or health of specific individuals.
- **Anonymised data** – personal data is not to be recorded or stored in a form that makes it possible to identify the data subject directly or indirectly.
- **Legitimate interest** – processing is necessary for the purpose of legitimate interest of the Controller, provided that no sensitive data is to be processed.

Lawful bases for disclosure of personal data

In addition to having a lawful basis for processing, a separate lawful basis is required when a Controller discloses personal data (e.g. disclosure of personal data to another legal entity – including within the same group).

Lawful bases for disclosure⁸ of personal data (Art. 15 of the PDPL)

- **Consent** – data subject has given consent to disclosure of his or her personal data.
- **Publicly available data** – personal data has been collected from a publicly available source.
- **Public interest or security purposes** – the entity requesting disclosure is a public entity, and the collection or processing of the personal data is required for public interest or security purposes, or to implement another law, to fulfill judicial requirements.
- **Public health and safety** – the disclosure is necessary to protect public health, public safety, or to protect the lives or health of specific individuals.
- **Anonymised data** – the disclosure will only involve subsequent Processing in a form that makes it impossible to directly or indirectly identify the data subject.
- **Legitimate interest** – the disclosure is necessary to achieve legitimate interests of the Controller, without prejudice to the rights and interests of the data subject, and provided that no sensitive data is to be processed.



⁸ Please note that in any case the Controller must comply with the restrictions on the disclosure, as they are specified in Art. 16 of the PDPL.

Rights of data subjects

The PDPL provides individuals with certain rights regarding processing of their personal data. The Controller must enable individuals to effectively exercise all such rights.

	Data subject right	Description of the right	Articles of the PDPL
01	Right to be informed	Data subjects have the right to be informed about the lawful basis and the purpose of collection of their personal data (for example via a privacy notice).	Art. 4 (1)
02	Right to access personal data	Data subjects have the right to access the personal data which is processed by the Controller.	Art. 4 (2)
03	Right to obtain personal data	Data subjects have the right to request their personal data to be provided to them in a readable and clear format.	Art. 4 (3)
04	Right to correct personal data	Data subjects can request to have their personal data corrected (if inaccurate), completed (if incomplete) or updated (if out of date).	Art. 4 (4)
05	Right to request destruction of personal data	Data subjects can request destruction of their personal data.	Art. 4 (5)
06	Right to withdraw consent	Data subjects may at any time withdraw their consent to processing of their personal data.	Art. 5 (2)
07	Right to submit a complaint to the Competent Authority	Data subjects may submit to the Competent Authority a complaint that may arise out of the implementation of the PDPL and the Regulations.	Art. 34

The Controller shall respond to the requests of the data subject pertaining to their rights under the PDPL within a period **not exceeding thirty (30) days** and without delay. This period may be extended by the Controller in case the response requires disproportionate effort, or if the Controller receives multiple requests from the data subject, provided that the extension does not exceed an additional (30) days and the data subject is notified in advance of the extension with the reasons for the delay.

In order to effectively respond to the above rights, a Controller should have in place, for instance, the following:

- a policy and procedure on responding to the rights of data subjects;
- a form for raising data subject requests (this could be for various channels);
- dedicated and trained data privacy team that can effectively respond to the rights of data subjects;
- technology tools that the data privacy team can use to respond to the requests of data subjects.

Get in Touch

To discuss how PwC can support you with implementing your data privacy programme, please get in touch.



Phil Mennie

Partner, Cybersecurity and Digital Trust

+971 56 369 7736

phil.mennie@pwc.com

[linkedin.com/in/philmennie](https://www.linkedin.com/in/philmennie) @philmennie



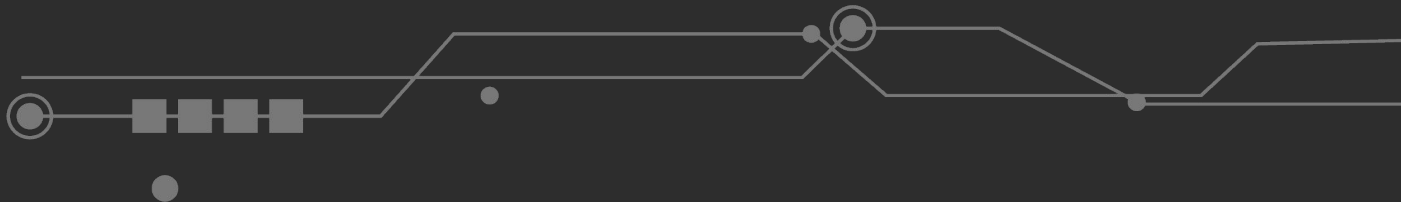
Richard Chudzynski

PwC Data Privacy Legal Leader

+971 56 417 6591

richard.chudzynski@pwc.com

[linkedin.com/in/richardchudzynski](https://www.linkedin.com/in/richardchudzynski)





Thank you

About PwC

Established in the Middle East for 40 years, PwC has 22 offices across 12 countries. As a community of solvers, with 8,000 people across the region, we bring the right combination of people, technology and expert capabilities from Strategy, through Advisory and Consulting to Tax and Assurance Services, to solve the region's most pressing challenges (www.pwc.com/me).

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.