Sultanate of Oman Personal Data Protection Law Series

Part 1 - Summary of the Law of Sultanate of Oman on Protection of Personal Data

pwc

Summary of the Law of Sultanate of Oman

Introduction

This “Sultanate of Oman Personal Data Protection Law Series” addresses the following:

- Summary of the Personal Data Protection Law (“**Law**”)
- Summary of the Executive Regulations of the Law (“**Executive Regulations**”)

On 13 February 2023 the Law came into force in the Sultanate of Oman (“**Oman**”). It is the main law in Oman regulating the use and processing of personal data.

The Executive Regulations came into force on 5 February 2024. However all entities in Oman have a grace period of one year - until 5 February 2025 - to ensure compliance with the Executive Regulations.

As a general rule, **all public and private entities** must comply with the Law and Executive Regulations.

The Ministry of Transport, Communications & Information Technology of Oman (“**Ministry**”) **is the competent authority which is responsible for enforcement of the Law and Executive Regulations.**

The Law provides fines (up to OMR 500,000) for breach of its provisions. The courts may impose fines from OMR 500 to OMR 500,000 and the Ministry may impose administrative fines up to OMR 2,000.

Key important notes

The Law in Oman has the following features that are not common to similar laws in the region (e.g. in Saudi Arabia and in the UAE):

- The Law provides for **only one legal basis** for processing of personal data - explicit consent of the data subject.
- The Law provides for a **substantial list of cases when the Law does not apply at all**. Among such cases are, for example, performance of a legal obligation, performance of a contract, processing of the data which is available in open sources, etc. Usually such cases are within the scope of personal data protection laws.
- The Law requires obtaining a **special permit for processing of personal data that is usually considered as sensitive** (e.g. health data).

Scope of the Law

What does the Law regulate?

The Law regulates processing[1] of personal data. The scope of the Law includes:

- processing of personal data of any type (e.g., contact information, health data, credit data, etc.);
- 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.);
- processing of personal data in any form (e.g., electronic or paper, structured or unstructured, etc.).

The personal data is defined in the Law as follows[2]: the data that would make a natural person identified or identifiable, directly or indirectly, in particular by reference to one or more identifiers, such as a name, an identification number, online identifiers or location data, or to one or more factors specific to the genetic, physical, mental, physiological, social, cultural or economic identity.

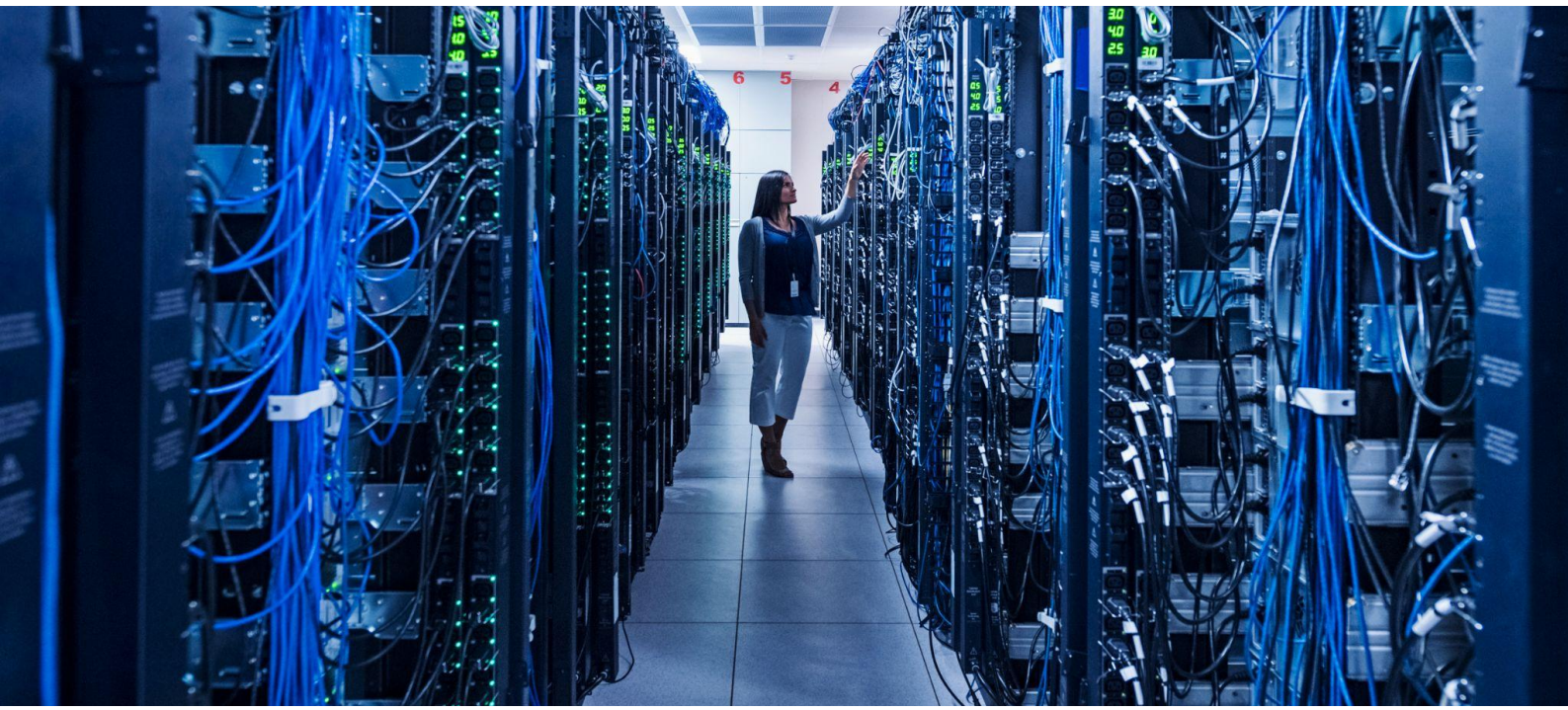
Therefore, any data based on which it is possible to identify an individual shall be considered as personal data under the Law. Examples would include an individual's name, telephone number, bank account number.

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 Law. Examples would include anonymized data, sales figures, data about the number of overall visits on the web page.

The Law does not provide a specific definition for sensitive data. However, Article 5 requires obtaining a permit from the Ministry to process the following categories of personal data:

01	Genetic data	05	Sexual life
02	Vital data (e.g. blood pressure and heart rate)	06	Political or religious beliefs
03	Health data	07	Criminal records
04	Ethnic origin	08	Data related to security measures.

Usually in personal data protection laws of other countries such categories of data are considered as sensitive data.



[1] "Processing" means any kind of use of personal data.
[2] Article 1 of the Law.

Roles and obligations of an entity under the Law

What are the roles that an entity can assume under the Law?

The Law 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 determines the purposes and means of the processing of personal data and conducts such processing on its own or delegates the processing to others entities on its behalf.

A Processor is an entity that processes personal data on behalf of the Controller.

What are the key obligations of the Controller?

Consent: The Controller must obtain consent of the data subject[3] before processing of personal data.

Controls and procedures: The Controller must establish controls and procedures for processing personal data, including for risk assessments, cross-border data transfers and technical measures to ensure compliance with the Law.

Privacy notice: Before processing personal data, the Controller must inform data subjects in writing about various aspects of the processing, including processing purpose, data source, processing procedures, etc.

[3] By “data subject” we mean any individual whose personal data could be processed.

What are the key obligations of the Controller? (continued)

Compliance with Ministry's controls: The Controller must comply with the controls and procedures Established by the Ministry to ensure that personal data is processed in compliance with the Law.

Cooperation with the Ministry: The Controller must cooperate with the Ministry by providing at its request the necessary data and documents.

Appointment of external auditor: Upon the Ministry's request, the Controller must appoint an external Auditor to verify compliance with processing procedures and controls. A copy of the auditor's report must be provided to the Ministry.

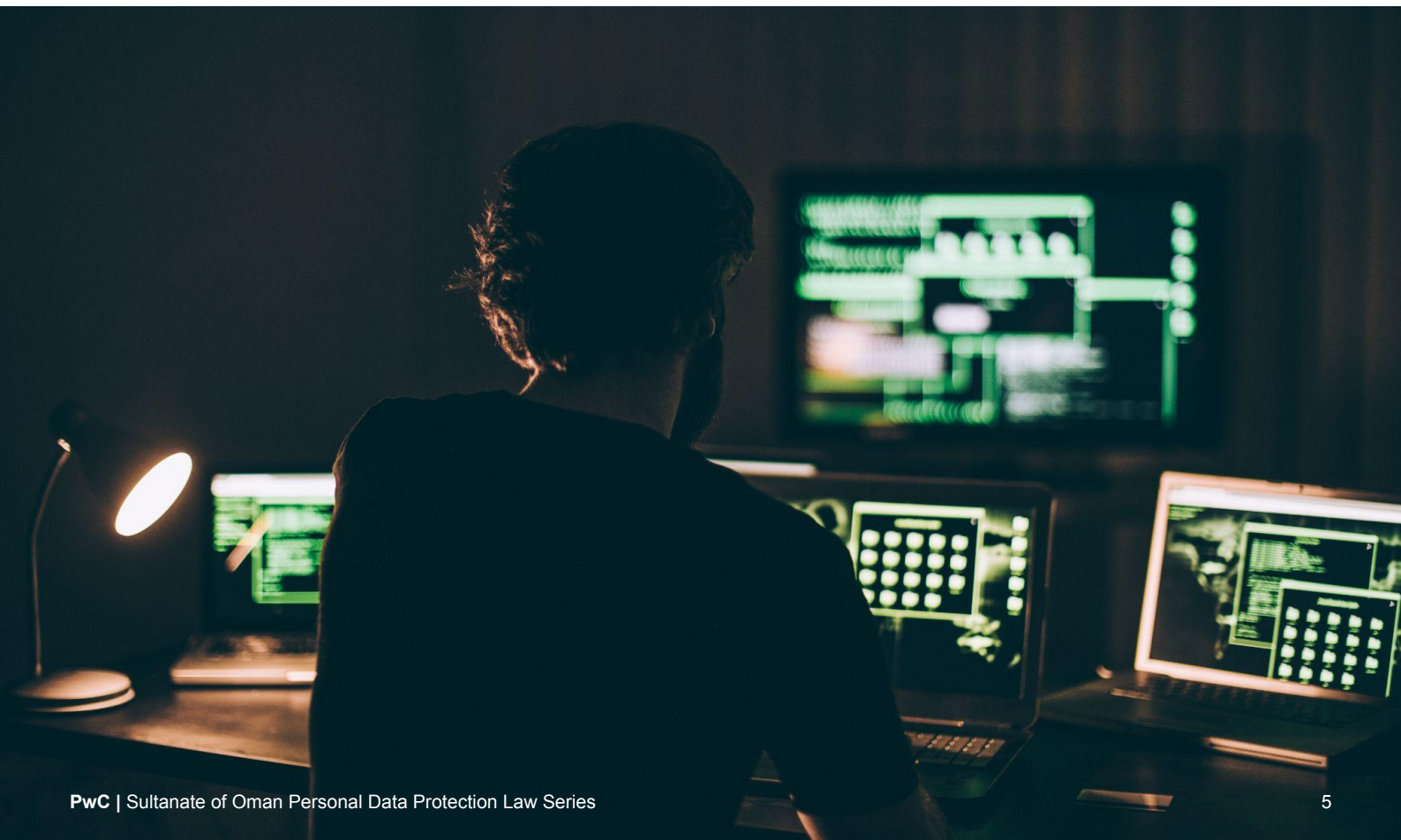
Document management: The Controller must keep the documents related to processing operations according to the timelines and procedures specified in the Executive Regulations.

Data breach notification: In case of a personal data breach, the Controller must notify the Ministry and the data subjects.

Appoint Data Protection Officer: The Controller must appoint the personal data protection officer according to the requirements of the Executive Regulations.

Confidentiality of personal data: The Controller must ensure the confidentiality of personal data and obtain prior consent from data subjects before publishing and disclosing their personal data.

Consent for advertising / marketing: Before sending any advertising or marketing materials with commercial purposes, the Controller must obtain written consent from the data subjects.



What are the key obligations of the Processor?

Compliance with Ministry's controls: The Processor must comply with the controls and procedures established by the Ministry to ensure that personal data is processed in compliance with the Law.

Cooperation with the Ministry: The Processor must cooperate with the Ministry by providing at its request the necessary data and documents.

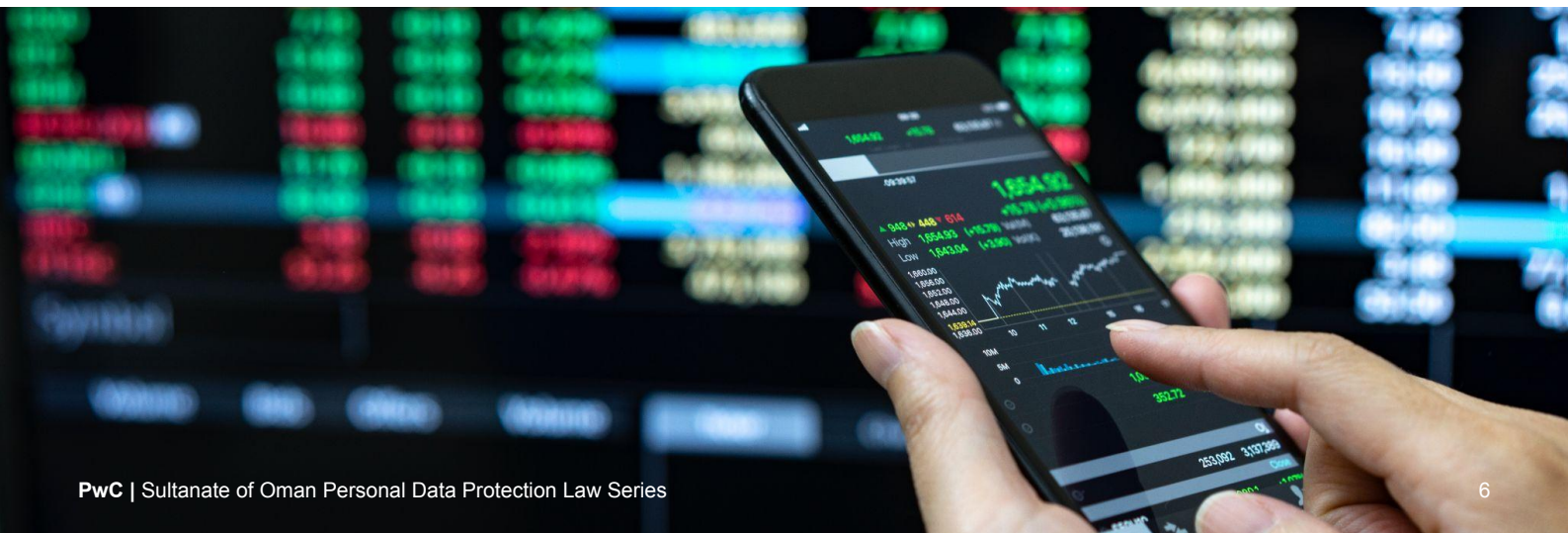
Appointment of external auditor: Upon the Ministry's request, the Processor must appoint an external auditor to verify compliance with processing procedures and controls. A copy of the auditor's report must be provided to the Ministry.

Document management: The Processor must keep the documents related to processing operations according to the timeline and procedures specified in the Executive Regulations.

Principles of personal data processing

The Law does not explicitly list any data protection principles. However there are certain important personal data protection principles that need to be taken into account by any organization processing personal data in Oman. Complying with these principles will also help complying with the Law.

No	Principle	Description of the principle
1	Lawfulness, fairness and transparency	Entity must: • ensure that it processes and discloses personal data only after obtaining consent from the data subject 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.
2	Purpose limitation	Entity must only process personal data for a specified and lawful purpose.
3	Data minimization	Entity must only process the personal data which it truly needs and nothing more.
4	Storage limitation	Entities must not keep personal data for longer than they need it (unless the longer storage is required by the laws).
5	Accuracy	Entity must ensure personal data is kept up to date, and that necessary measures are in place for correcting and updating inaccurate data.
6	Integrity and confidentiality	Entity must implement adequate security controls to ensure that personal data is protected against loss, destruction or damage.
7	Accountability	Entity must have appropriate measures and records in place to be able to demonstrate compliance with the Law.

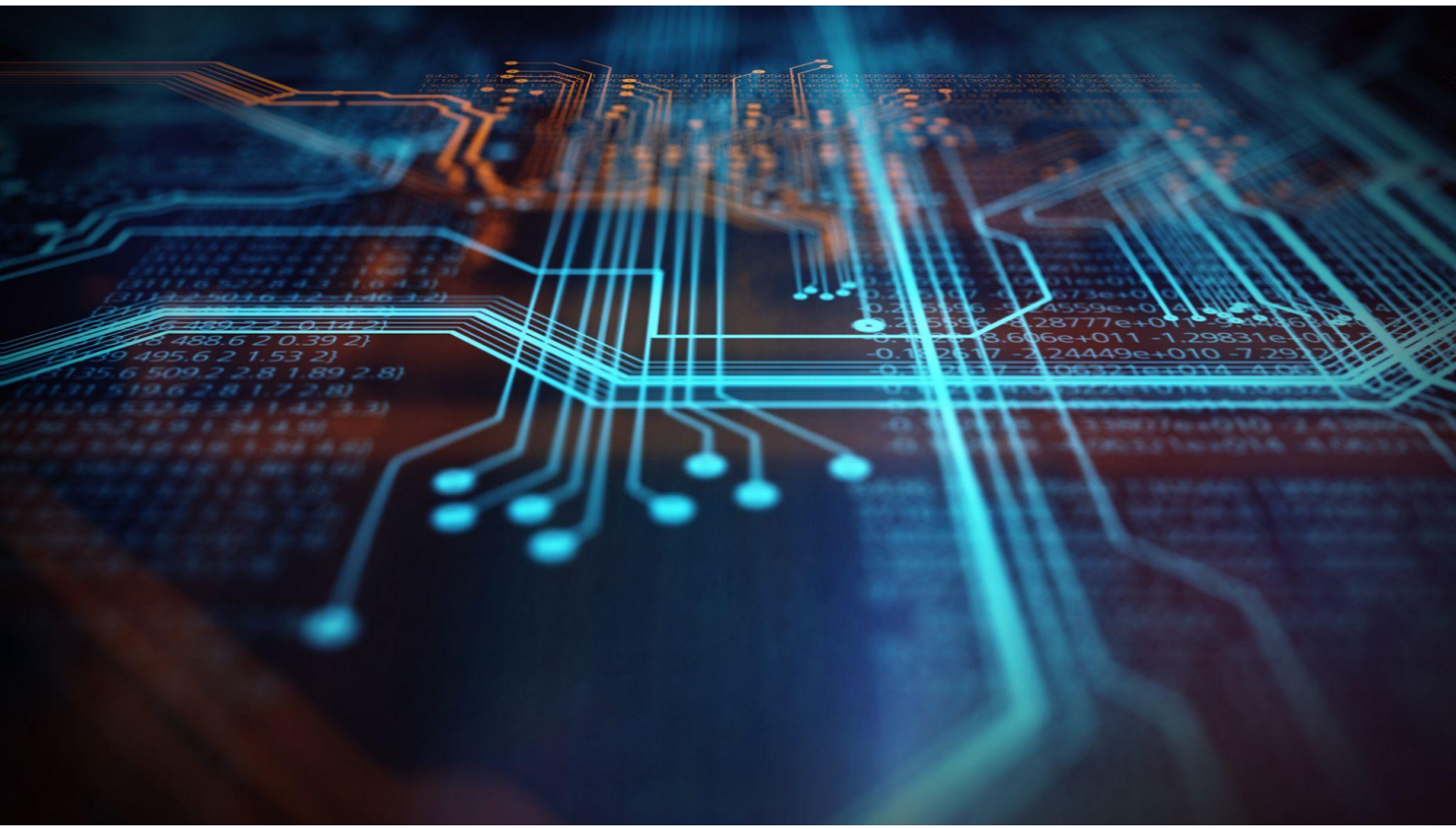


Lawful basis for personal data processing

The Law provides for **only one lawful basis for processing of personal data** - explicit consent of the data subject. That said, the Law provides for a number of cases, when the provisions of the Law (including the requirement to the written explicit consent) shall not apply:

Exceptions (under Art. 3 of the Law)

- Protection of national security or public interest.
- Performance of the units of the administrative apparatus of the state and other public legal persons of the powers prescribed for them by law[4].
- Performance of a legal obligation imposed upon the Controller under any law, judgment, or court decision.
- Protection of the economic and financial interests of the country.
- Protection of a vital interest of the data subjects.
- Detection or prevention of any crime based on an official written request from the investigation authorities.
- Performance of a contract to which the data subject is a party.
- If the processing is in a personal or confidential context.
- If the processing is performed for the purposes of historical, statistical, scientific, literary, or economic research by the authorities authorized to carry out such research, provided that no indication or reference related to the data subjects is used in the research and statistics to be published, so that the personal data is not attributed to an identified or identifiable natural person.
- If the data is available to the public and in a manner that does not violate the provisions of the Law.



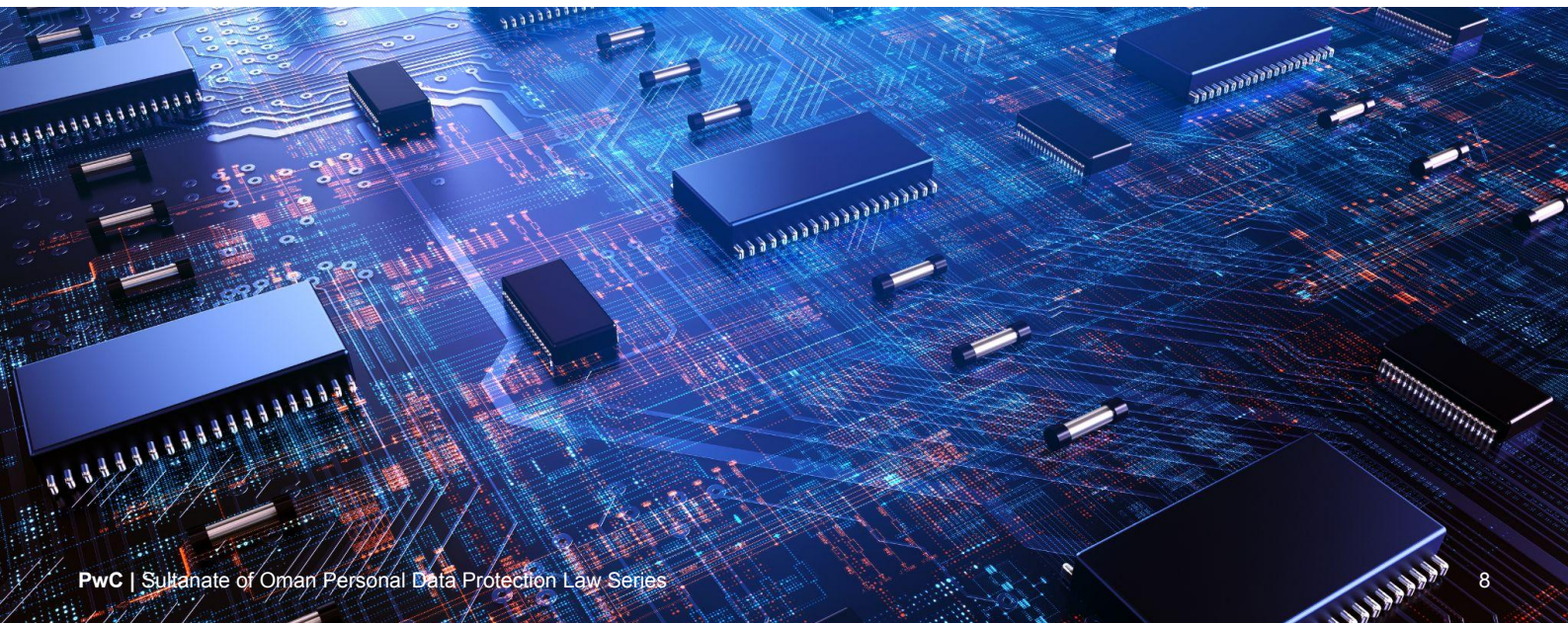
[4] In April 2024 the Ministry issued a Personal Data Protection Policy of the Units of the Administrative Apparatus of the State. Such units shall process personal data in compliance with this policy.

Rights of data subjects

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

No	Data Subject Right	Description of the right	Articles of the Law
1	Right to be informed	Data subjects have the right to be informed about the purpose of processing of their personal data, as well as about other aspects of such processing (as specified in Art. 14 of the Law).	Art. 14
2	Right to access the personal data	Data subjects have the right to access the personal data which is processed by the Controller.	Art. 14 (e)
3	Right to withdraw consent	Data subjects have the right to revoke their consent to the processing of their personal data.	Art. 11 (a)
4	Right to correct the personal data	Data subjects have the right to request to have their personal data corrected (if inaccurate) or updated (if out of date).	Art. 11 (b)
5	Right to block personal data	Data subjects have the right to request the Controller to block their personal data and, thus, restrict its processing.	Art. 11 (b)
6	Right to obtain a copy of the personal data	Data subjects have the right to obtain a copy of their personal data which is being processed.	Art. 11 (c)
7	Right to transfer personal data	Data subjects have the right to request the Controller to transfer their personal data to another Controller.	Art. 11 (d)
8	Right to erasure of the personal data	Data subjects have the right to request the erasure of their personal data unless such processing is necessary for national records-keeping or documentation purposes.	Art. 11 (e)
9	Right to be notified about the breach	Data subjects have the right to be notified of any breach or violation regarding their personal data and the measures taken in this regard.	Art. 11 (f)

More details on the requirements of the Law are provided in the Executive Regulations to it. Please see the summary of the Executive Regulations in part 2 of the Sultanate of Oman Personal Data Protection Law Series.



Get in Touch

To discuss how PwC can support you in personal data protection compliance, please get in touch.

Phil Mennie
Partner, Cybersecurity and Digital Trust
+971 56 369 7736
phil.mennie@pwc.com
linkedin.com/in/philmennie @philmennie

Nayaz Mohammed
Partner, Digital Trust
+968 9942 9679
nayaz.mohammed@pwc.com
linkedin.com/in/nayaz-mohamed-37aa966/

Richard Chudzynski
PwC Data Privacy Legal Leader
+971 56 417 6591
richard.chudzynski@pwc.com
linkedin.com/in/richardchudzynski

Abdullah Al Busaidi
Manager, Digital Trust
+968 7911 2217
abdullah.albusaidi@pwc.com
linkedin.com/in/abdullah-albusaidi/

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).