Sultanate of Oman Personal Data Protection Law Series

Part 2 - Summary of the Executive Regulations to the Law of Sultanate of Oman on Protection of Personal Data

pwc

Introduction

On 13 February 2023 the Personal Data Protection Law ("**Law**") came into force in the Sultanate of Oman ("**Oman**"). It is the main law in Oman regulating the use of personal data.

On 5 February 2024 the Executive Regulations to the Law ("**Executive Regulations**") came into force in Oman. The Executive Regulations provide further details to the existing requirements of the Law. In principle it does not change the key concepts and requirements of the Law. Please see Part 1 of our series for details on the Law.

All entities in Oman have a grace period of one year - until 5 February 2025 - to ensure compliance with the Executive Regulations.

Key Requirements of the Executive Regulations

Governance

The Controller[1] must appoint a personal data protection officer ("**DPO**"), according to the following requirements:

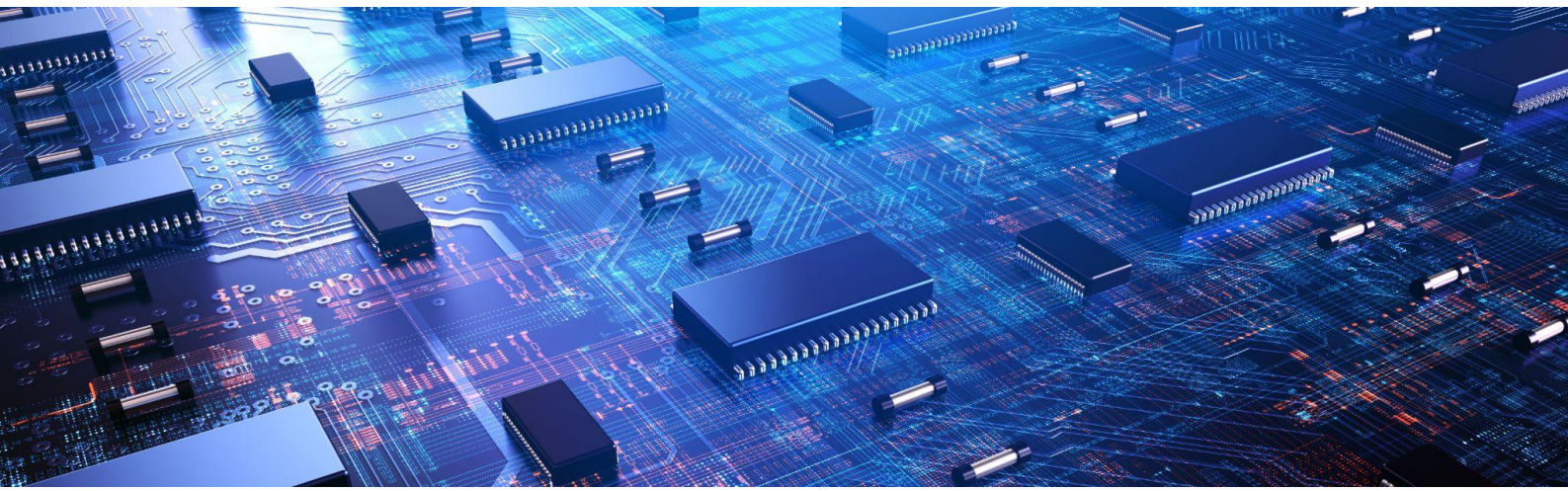
- DPO must be qualified to carry out the tasks stipulated in Art. 35 of Executive Regulations (e.g. providing consultations to the Controller or the Processor regarding their obligations under the Law and the Executive Regulations, etc).
- To be familiar with the Law and Executive Regulations, as well as the personal data protection practices carried out by the Controller or the Processor.
- To be professionally competent and capable of dealing regularly and correctly with all issues related to the protection of personal data.

Art. 34

The DPO is responsible for the following:

- Providing proposals and consultations to the DPO's organization regarding its obligations under the Law and Executive Regulations.
- Control performance by the organization of its obligations under the Law and Executive Regulations.
- Control implementation of the organization's policies related to the protection of personal data.
- Coordination with the competent department of the Ministry of Transport, Communications & Information Technology of Oman **("Ministry")**[2] on matters related to the processing of personal data.

Art. 35



[1] Please see explanation of the key concepts of the Law (e.g. Controller, Processor, etc.) in part 1 of the Sultanate of Oman Personal Data Protection Law Series.

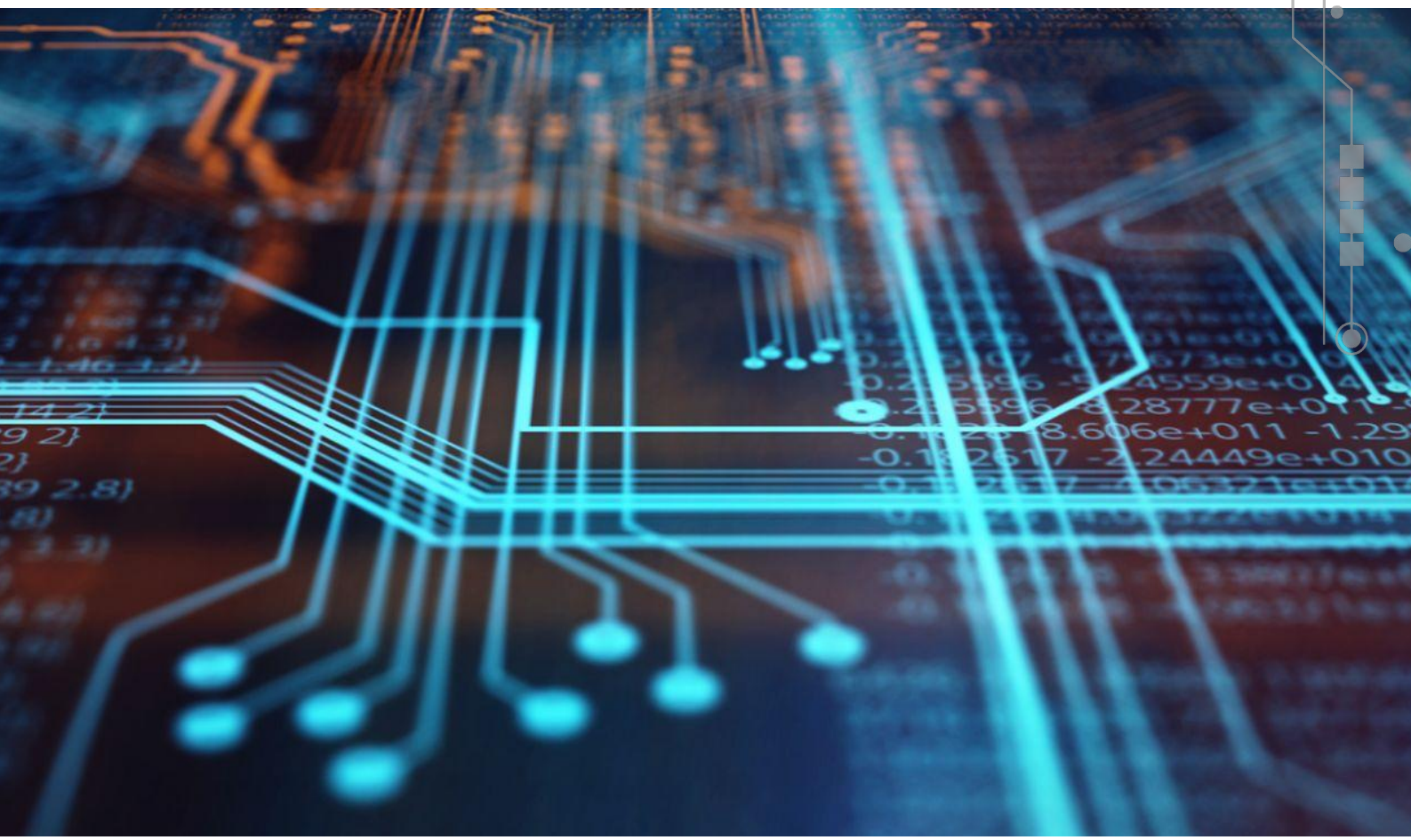
[2] The Ministry is the competent authority in the area of personal data protection in Oman. The "competent department" is the department in the Ministry that is responsible for managing the issues related to personal data protection.

The Controller must publish the information about the DPO, including his / her name and contact details (this could be done in the company's privacy notices). Data subjects must also be able to contact the DPO on all matters related to the processing of their personal data.

Art. 36

The Controller or the Processor - as the case may be - must publish a personal data protection policy[3] in a visible location that allows the data subject to inspect it before their personal data is processed. This policy should include at least the mechanism and procedure for exercising the data subject rights specified in the Law and Executive Regulations.

Art. 21



Cooperation with the Ministry

The Controller or Processor (depending on the circumstances) must provide the Ministry with any documents, data or any additional information within 30 days from the date when such information could be requested by the Ministry.

Art. 2

[3]From the context of the Executive Regulations it seems this requirement refers to a privacy notice and not personal data protection policy (internal document of organization).

Data subject rights

Please see the list of the data subject rights in part 1 of the Sultanate of Oman Personal Data Protection Law Series.

The personal data subject may submit a written request to the Controller to exercise any of his rights stipulated in Art. 11 of the Law, free of charge. The Controller must decide on the request within a period not exceeding 45 days from the date of its receipt.

In some cases the Controller may refuse to fulfill the request of the data subject (e.g if the request is unjustifiably repetitive or its fulfillment requires extraordinary effort).

Art. 16, Art. 17

The Executive Regulations provide for additional details on how the Controller shall ensure that the data subjects can exercise their rights.

For instance, the data subject has the right to request the erasure of his personal data (which is held by the Controller) in any of the following cases:

- If the purpose of processing has been completed.
- If the data subject revokes his / her consent to the processing of his / her personal data.
- If the data processing does not comply with the provisions of the Law and Executive Regulations.

The Controller may - depending on the circumstances - reject the data subject's request to erase the personal data in the following cases:

- Implementing a legal obligation imposed on the Controller under any law, ruling or judicial decision.
- There is an ongoing dispute between the Controller and the data subject.

Art. 18

The data subject has the right to request from the Controller a copy of his / her processed personal data in a readable and clear electronic or paper format, provided that he ensures that the copy he provides does not contain any personal data that identifies another person.

Art. 19

The data subject has the right to transfer his or her personal data to a new Controller. The Controller shall transfer the personal data to the new Controller if there is a legal obligation to do so.

Art. 20

Consent and processing for marketing communication

Before processing personal data, the Controller is obligated to obtain the explicit consent of the data subject. The following conditions must be complied with in relation to the consent:

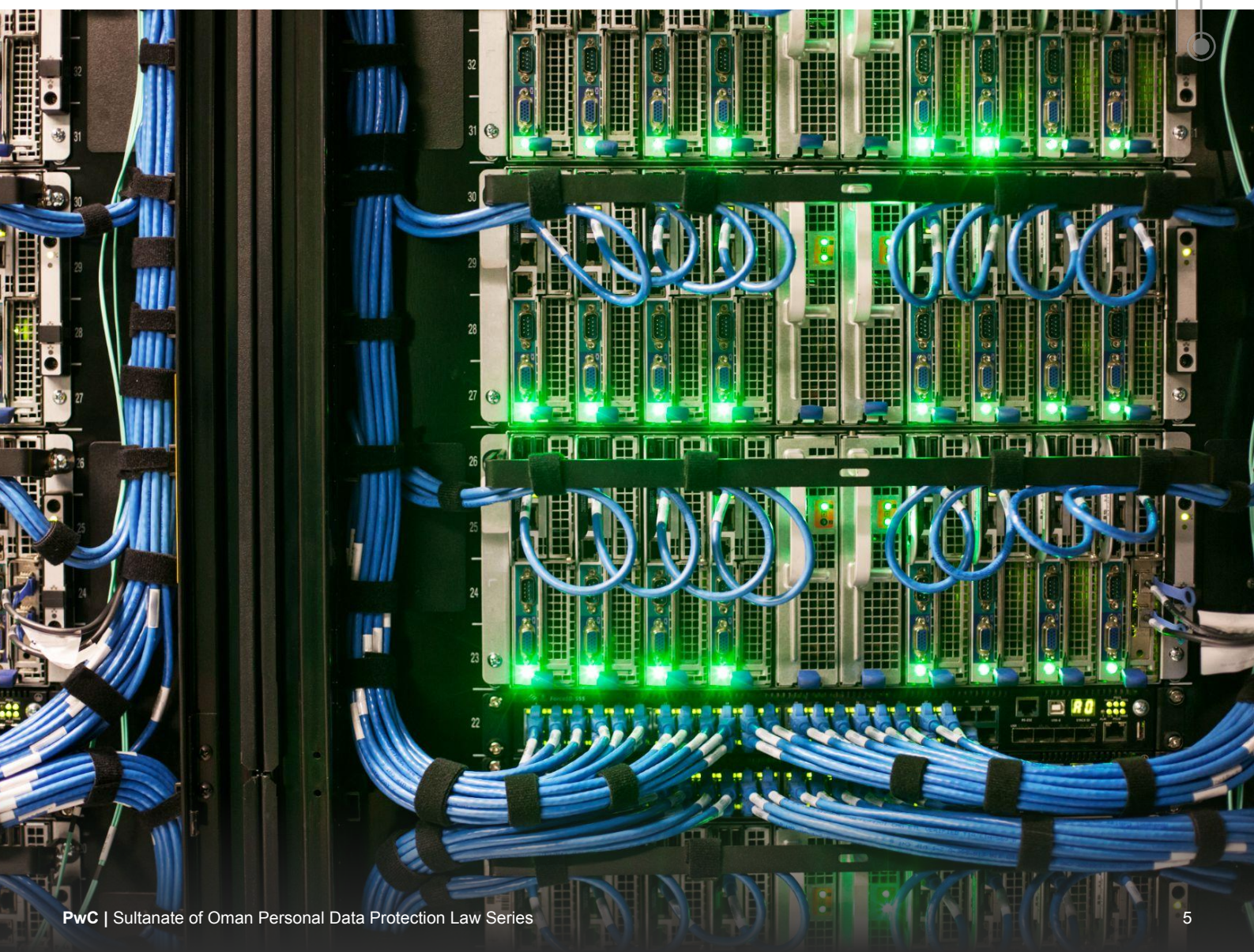
- The consent must be issued by a legally competent person.
- Consent must be issued in a clear manner and without coercion.
- The approval must be in writing, in an electronic form, or made by any other means determined by the Controller.

Art. 4

The Controller must, prior to sending any advertising, marketing or commercially-purposed communications to the data subject, comply with the following:

- Obtain the written consent of the data subject.
- Notify the data subject of the channels used for sending advertising, marketing or commercial communications.
- Identify a mechanism to stop receiving advertising, marketing or commercial communications.
- Immediately suspend any advertising, marketing or commercial communications upon receiving a suspension request from the data subject free of charge.

Art. 22



Data Lifecycle Management

The Executive Regulations specify requirements for maintenance of the records of processing activities ("**RoPA**"). The Controller and the Processor (as the case may be) shall maintain the RoPA and shall include the following information to it:

- Data of the DPO (name, contact details, etc.).
- Description of categories of personal data the Controller / the Processor maintains, as well as the details of the persons authorized to access the personal data.
- Processing time periods, restrictions and scope of processing.
- The mechanism for erasing, modifying or processing personal data.
- The purpose of processing personal data.
- The entities to which personal data is disclosed and the purposes of disclosure.
- Data of any entity to which personal data is transferred.
- Any data related to the movement and processing of personal data outside the borders of Oman.
- Technical and organizational procedures related to information security and processing operations.
- Any personal data breaches, including the facts related to the breach, its effect, as well as the remedial or corrective action taken.

Art. 28

The Controller must update the RoPA on an ongoing basis and submit it to the competent department of the Ministry whenever it requests the RoPA.

Art. 29

Data breach management

The Executive Regulations provide for details on the obligation of the Controller to notify the Ministry and data subjects of a personal data breach.

For instance, the Controller must inform the competent department of the Ministry within a period not exceeding 72 hours from the time the Controller became aware of the breach if such a breach would result in a risk to the rights of data subjects.

The notification must include - at a minimum - the following information:

- Description and details of the nature of the breached data and the consequences of the breach.
- Data and contact information of the Controller or any other contact point, from whom the data subject may obtain more information.
- A description of the potential effects of the breach.
- Corrective measures or technical and organizational measures that the Controller will take to address the breach, including - when necessary - proposed measures to mitigate the potential negative effects.
- Corrective actions, as well as technical and organizational measures taken by the Controller immediately upon becoming aware of the breach and before informing the competent department of the Ministry.

Art. 30

The Controller shall notify the data subjects within a period not exceeding 72 hours from the time the Controller became aware of the breach. The notification is required only if such a breach is likely to result in significant damage or a high risks to the data subject.

The notification to data subjects must include – at a minimum – the following information:

- Type and nature of the breach.
- Details of the personal data that was impacted by the breach.
- Recommendations on how to limit or mitigate the impact of the breach, if necessary.

Art. 32

Cross-Border Data Transfer

Before transferring personal data outside the borders of Oman, the Controller must obtain the express consent of the data subject. The transfer of personal data must not impact national security or the interests of the state.

Obtaining the consent of the data subject is not required in one of the following cases:

- The transfer of personal data is performed in implementation of an international agreement to which Oman is a party.
- The transfer is performed in a way that leads to anonymization of the data subject, not linking this personal data to him / her and not being able to identify him in any way.

Art. 37

Before transferring personal data outside the borders of Oman, the Controller must ensure that the external processing party (receiver of the personal data) can provide a level of protection for personal data that is not less than provided under the Law and Executive Regulations.

Art. 38

The Controller must conduct an assessment of the level of protection provided by the external processing party, as well as of the risks related to the transfer of personal data. The assessment shall include the following:

- A description of the nature and size of the personal data to be transferred and the degree of its sensitivity.
- The purpose of processing personal data, the scope of processing, and the parties with whom the personal data will be shared.
- The time period for processing personal data, and whether it will be done in a restricted or occasional manner, only once, or repeatedly and regularly within a limited period of time.
- The stages of the transfer of personal data, the countries it may pass through, as well as the final destination of the personal data.
- The effects and risks that may result from the transfer of personal data, as well as the extent of their impact on the data subjects.

Art. 39

The Ministry may request a copy of the assessment report prepared by the Controller.

Art. 40

Permit for processing sensitive data

The Law requires that before processing any sensitive data (as described in Art. 5 of the Law) the Controller must obtain a permit from the Ministry. The Executive Regulations provide for the procedure on obtaining such a permit.

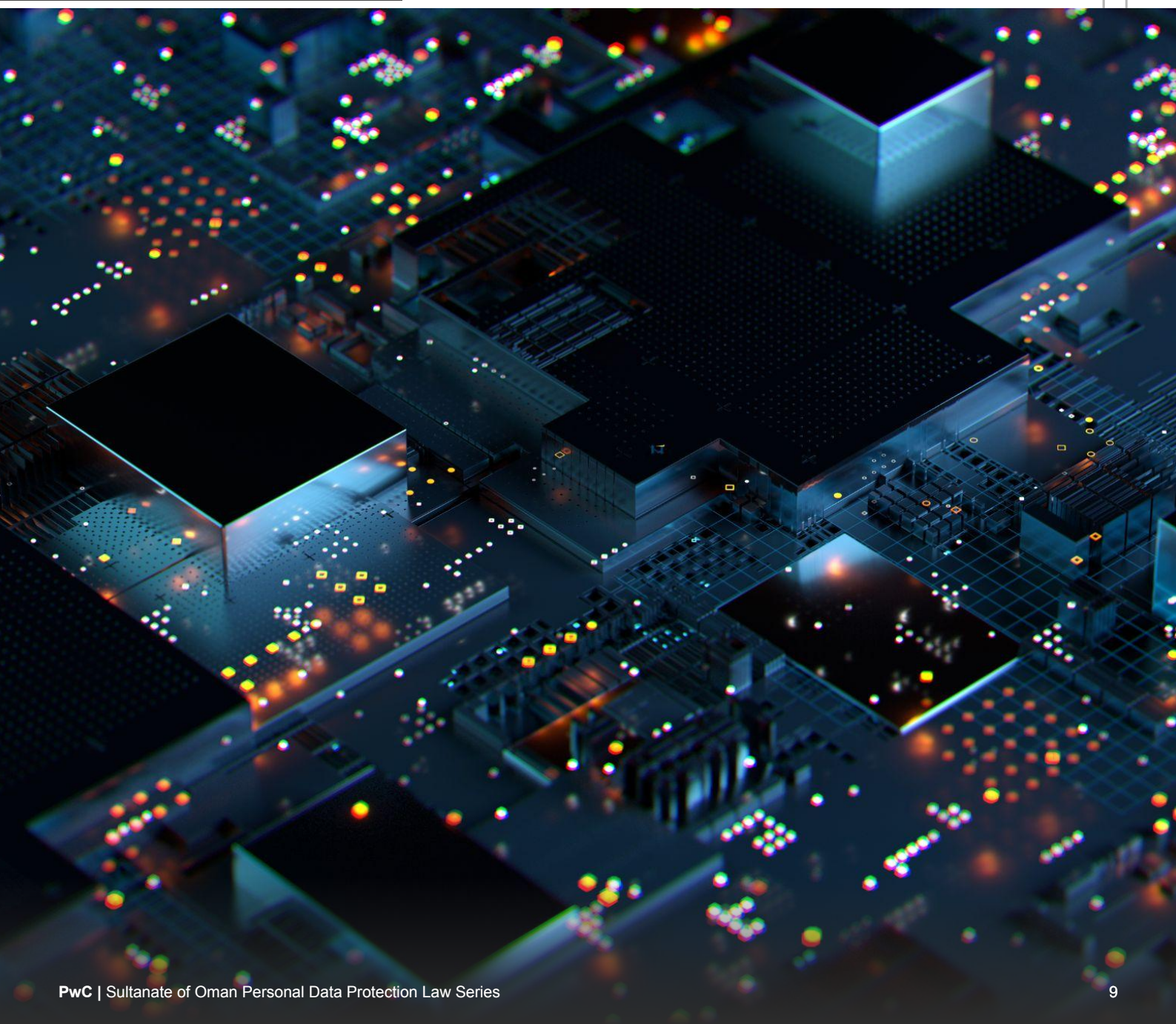
The Procedure includes the following:

Step 1: The Controller submits an application to the Ministry. The Controller must attach to the application its personal data protection policy and description of the measures regarding response to the personal data breach.

Step 2: The Ministry must make a decision on granting the permit within 45 days after receiving all information and documents from the applicant. If the Ministry rejects the application, the Ministry must provide the reasons for such a rejection. Failure by the Ministry to respond within 45 days shall be considered as a rejection of an application. The applicant may make an appeal regarding the rejection.

Step 3: The permit shall be issued by the Minister for a period not exceeding 5 years. The permit shall be renewed for a similar period, in accordance with the same procedure.

Art. 5 - Art. 8



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).