

DENTONS

Oman Personal Data Protection Law

Presented by Fatima Al Sabahi and Simon Topping

Grow | Protect | Operate | Finance

Outline

- 1 Introduction
- 2 Key terms
- 3 Scope
- 4 Requirements
- 5 Complaints and enforcement
- 6 Summary
- 7 Q&A



Presenters



Fatima Al-Sabahi
Senior Associate, Muscat



Simon Topping
Senior Legal Consultant, Muscat

Introduction

This presentation will help you better understand:

- Oman's personal data protection legislation
- your rights and obligations
- the risks in not complying with the law



A scenic mountain landscape with a blue overlay. The background shows a range of jagged, rocky mountains under a clear sky. The foreground is a rocky, uneven terrain. A large, semi-transparent blue shape covers the left and center of the image, with a white text overlay.

Key terms

Key terms


What is “personal data”?

“Data that identifies a natural person or makes such person identifiable, directly or indirectly, by reference to identifiers such as name, civil number, electronic identifier data or address related data or factors such as genetic, physical, mental, physiological, social, cultural or economical identity”

Key terms

Who is protected?

- “Person who the personal data relates to” (صاحب البيانات الشخصية) = “Data Subject”



“Any natural person who can be identified from their personal data”

Key terms

Who is responsible for protecting personal data?

Controller

person responsible for specifying the purpose and method of processing personal data

Processor

person responsible for processing the personal data on behalf of the Controller

Key terms

Processing

an operation or a set of operations performed on personal data including: collecting, recording, analysing, organising, storing, adapting, altering, retrieving, reviewing, formatting, combining, blocking, erasing, cancelling, or disclosing it by transmission, dissemination, transfer, forwarding or making it available otherwise

The background features a close-up of a corn cob with water droplets on its kernels. A large teal shape, resembling a stylized arrow or a leaf, is overlaid on the image, pointing towards the right. The word "Scope" is written in white, bold, sans-serif font on the left side of the teal shape.

Scope

Key personal data protection legislation in Oman

- Personal Data Protection Law, promulgated by Royal Decree 6/2022 (**PDPL**)
 - came into force on 13 February 2023
- Ministerial Decision no. 34/2024 executive regulations to the PDPL issued by (**Executive Regulations**)
 - came into force on 5 February 2024
 - one year grace period
- Ministry of Transport, Communications and Information Technology (**Ministry**) is the personal data protection regulator through its Personal Data Protection Department

Exceptions to PDPL

Article 3 of the PDPL

- Protection of national security or the public interest
- Performance by the units of the administrative apparatus of the State and other public legal persons of the competencies prescribed for them by law
- Performance of a legal obligation imposed on the Controller under any law, judgment or decision of a court
- Protection of the economic and financial interests of the state
- Protection of a vital interest of the Data Subject
- Detection or prevention of any criminal offense based on an official written request from the authorities
- Executing a contract to which the Data Subject is a party
- Processing in a personal or family context
- If the data is available to the public in a manner that does not violate the provisions of the law

The background features a soft-focus photograph of tall grasses against a warm, golden sunset sky. A large, semi-transparent blue shape with a rounded right edge is overlaid on the left and center of the image. The word "Requirements" is written in white, bold, sans-serif font within this blue area.

Requirements

Data Controller and Processor

The Controller and / or Processor are responsible for complying with the requirements of personal data protection depending on the obligation





Requirements prior to processing

- Controller must obtain express consent of the Data Subject before processing personal data:
 - request for processing personal data must be written in a clear, explicit and understandable manner
 - consent to process personal data must be in writing, electronic or by any other means decided by the Controller

Rights of Data Subjects

Article 11 of the PDPL

Data Subjects have the right to:

- revoke their consent to the processing of their personal data
- request for their personal data to be amended, updated or blocked
- obtain a copy of their processed data
- request the transfer of their personal data to another controller
- Request erasure
- be notified of any breach or infringement of their personal data





Requirements resulting from Data Subject rights

- Controllers and Processors must have processes and procedures to ensure that Data Subjects can exercise the data subject rights under the law
 - Written request from Data Subject (halt processing)
 - Controller must respond in 45 days
 - Controller can refuse if unjustifiably repetitive or extraordinary effort
 - Erasure if purpose completed, revoke consent, non-compliance, unless legal obligation, dispute
 - Copy of personal data in readable and clear electronic or paper format

Requirements – information that must be given to Data Subjects

- Controller must ensure there is a mechanism to notify all Data Subjects of required information before processing including:
 - Identity of the Controller and the Processor
 - Contact information of the Data Protection Officer
 - Purpose of the personal data processing and the source from which it is collected
 - Comprehensive description of processing and procedures and the degree of disclosure of personal data
 - Data Subject rights
 - Any other information that may be necessary to fulfil the processing conditions

Requirements – display requirement for processing

- Controller / Processor must:
 - place a Personal Data Protection Policy in a visible place that allows the Data Subject to view it before processing their data
 - include at least the mechanism and procedures for the Data Subjects to exercise their rights
- Note the overlap



Requirements – data breach

- If there is a data breach (unlawful access to Personal Data in a way that leads to its unlawful destruction, alteration, disclosure, access or processing e.g. personal data being extracted through a hack), then:
 - Controller must inform the **Ministry** within 72 hours from the time they are aware of a breach if it would lead to a threat to a Data Subject's rights. The report must contain certain specified information.
 - Controller must inform the **Data Subject** within 72 hours from being aware of the breach if it would cause serious harm or high risk to the Personal Data Subject. The report must contain specified information.
- As a practical matter you should establish a data breach procedure and draft notification forms to comply with the above obligations

Requirements – Data Protection Officer

- Controller must appoint a Data Protection Officer (**DPO**) who is:
 - Qualified to carry out the tasks specified in the Regulations
 - Familiar with the PDPL/Regulations and the data protection practices of the Controller or the Processor
 - Competent: professional, and able to deal, regularly and correctly, with all issues related to the data protection
- An employee may be appointed as a DPO even if they have other duties
- Controller must publish information relating to the DPO, including their name and contact information, by any means, and the Data Subjects have the right to contact the Personal Data Protection Officer on all issues related to the Personal Data Processing

Requirements – confidentiality/security

- Controller must ensure confidentiality and that there is no publication of personal data without the prior consent of the Data Subject, by:
 - establishing, using and activating electronic systems for protection against illegal access, leakage, tampering with or misuse of Personal Data
 - establishing systems to recover Personal Data when a physical or technical accident occurs
 - having effective testing processes for its existing technical procedures

Requirements - record of data processing

- The Controller/ Processor must keep a record of data processing (and update it) including:
 - Identity of the Data Protection Officer
 - Categories of personal data and the persons authorized to access personal data
 - Processing deadlines, restrictions and scope
 - Mechanism for deletion, modification or processing personal data
 - Purpose of processing
 - Data of any entity to which personal data is transferred or transmitted
 - Trans-border transfer information
 - Technical procedures for Information Security and Processing Operations
 - Any personal data breach incidents and corrective action taken

Requirements – direct marketing

- Before sending any advertising, marketing or commercial material to the Data Subject, the Controller must:
 - Inform the Personal Data Subject of the means of sending advertising, marketing or commercial materials
 - Obtain the written consent of the Personal Data Subject
 - Determine the process for suspension of sending advertising, marketing or commercial materials
 - Suspend sending advertising, marketing or commercial materials immediately upon receiving a suspension request from the Data Subject without compensation



Requirements – data retention policy

- The Controller / Processor must establish and comply with a data retention policy detailing processing operations and the purpose for document retention which must comply with the law:
 - reason for keeping processing must be specific and lawful
 - retention period must be determined according to the purpose of processing
 - technical protection systems must be provided for the safe preservation of processing documents

Processing Sensitive Data

Sensitive Data is data about an individual's:

- Race or ethnic origin
- Political opinions
- Religious beliefs
- Health data
- Genetic data
- Biometric data
- Sexual life
- Criminal convictions

Sensitive Data also includes data about security measures



The image shows the silhouettes of several tall, thin grasses with feathery seed heads against a soft, warm, orange-hued sky, likely during sunrise or sunset. The grasses are positioned in the lower half of the frame, with their stems extending upwards. The sky is a uniform, light orange color, creating a serene and natural background.

Requirements if processing Sensitive Data

- The Controller must apply for a permit from the Ministry to process Sensitive Data



Requirements for transferring personal data outside Oman

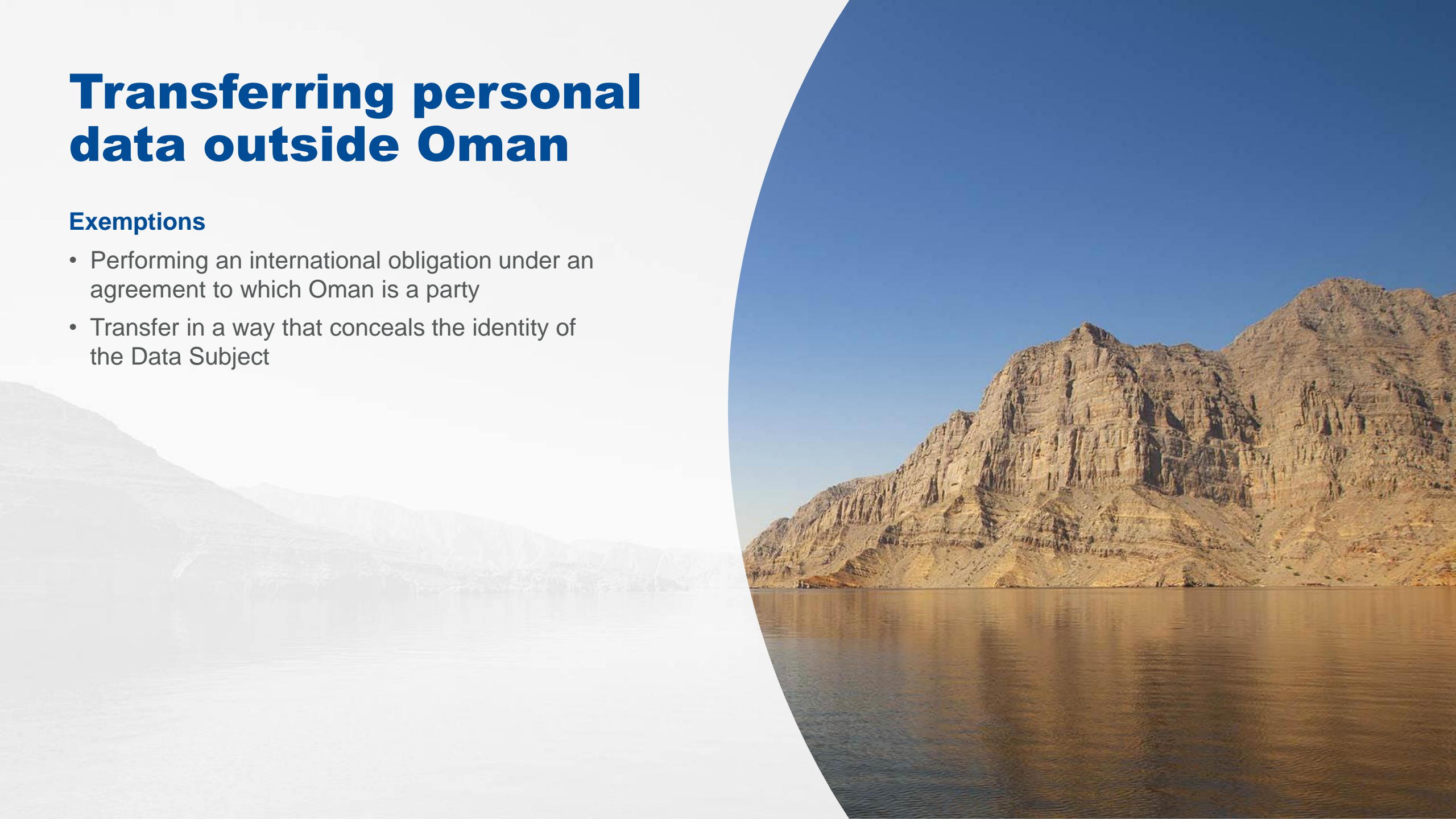
Controller must:

- obtain the express consent of the Data Subject before the transfer
- ensure that the data transfer does not jeopardise national security or the interests of the country
- ensure the receiving country has adequate protection measures that are no less than Oman law

Transferring personal data outside Oman

Exemptions

- Performing an international obligation under an agreement to which Oman is a party
- Transfer in a way that conceals the identity of the Data Subject



Requirements – processor assessment

- Controller needs to conduct an assessment for third party processors
 - Description of the nature and size of the Personal Data to be transferred or moved, and the degree of its sensitivity
 - The purpose of processing Personal Data, the scope of Processing, and the parties with whom the it will be shared
 - The time 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
 - The stages of transferring or moving Personal Data, the States it may pass through, and determine the final destination of the Personal Data
 - The effects and risks that may result from the transfer or movement process, and the extent of their impact on the Data Subject

Requirements – other procedures specifically mentioned

- Controller must establish controls and procedures including:
 - To determine risks that may fall on the Data Subject as a result of processing
 - Procedures for the transfer of personal data outside of Oman
 - Technical procedures to ensure that the processing is carried out in accordance with the law



Auditor

The Controller and the Processor must appoint an auditor if requested by the Ministry to audit the processing of personal data and confirm it is in accordance with the law





Complaints & Enforcement



Complaints

- A Data Subject must file a complaint with the Ministry within 30 days of becoming aware of the infringement
- The Ministry must (i) inform the Controller within 7 days of receiving the complaint; and (ii) give the Controller 14 days to respond
- The Ministry has 60 days to address the complaint. If it does not respond within this time-frame, then it is deemed a rejection

Penalties

The Ministry can:

- issue a notice of violation
- suspend a permit until the violation is remedied
- impose an administrative fine for certain violations not exceeding OMR 2,000 per violation
- impose a fine for a violation that constitutes a criminal offence under the PDPL ranging from OMR 500 and OMR 500,000
- cancel the Controller's processing permit



The background features a soft-focus image of pink cherry blossoms against a light blue sky. A dark green, semi-transparent overlay covers the left and bottom portions of the image, with a rounded corner on the right side. The word "Summary" is written in white, bold, sans-serif font on the green overlay.

Summary

Summary

Requirements on Controllers and to some extent Processors are significant including:

- various consent requirements to be obtained from data subjects for processing and transfer outside of Oman (express), direct marketing (written)
- information to be given to Data Subjects before processing and direct marketing, and display obligation
- appointment of DPO
- permit requirement for Sensitive Data
- policy for data retention
- processor assessment
- processes and controls to deal with Data Subject rights, data breach, DPO, confidentiality/security, direct marketing, transfer abroad/to a processor, document/data retention



Q & A