Baker McKenzie.

Client Alert

September 2026

Oman: Strengthening Its Data Protection Regime

New rules extend overseas reach and regulate automated decision-making

In brief

Oman has significantly amended its Personal Data Protection Law (PDPL) through Royal Decree No. 68/2026, marking the most substantial update to the country's privacy framework since the law was enacted in 2022. The amendments took effect on 7 September 2026 and introduce a number of changes that will be particularly relevant for international businesses processing personal data relating to individuals in Oman.

The reforms expand the territorial scope of the law, introduce new circumstances in which personal data may be processed without obtaining explicit consent, establish a framework for automated processing and automated decision-making, and create additional flexibility for certain employment- and security-related processing activities.

The changes bring several aspects of the Omani regime closer to international privacy standards, including concepts familiar under the EU General Data Protection Regulation (GDPR). However, Oman retains a number of unique features, particularly in relation to sensitive data, government oversight and cross-border transfers.

For multinational organisations operating regional or global processing models, the amendments may significantly broaden the number of activities that fall within scope of the Omani privacy regime.

Contents

Key takeaways

The amendments introduce several important developments for businesses:

- **The PDPL now expressly applies to processing activities taking place outside Oman**, creating a broader extraterritorial reach for organisations handling personal data relating to individuals in Oman.
- **Consent is no longer the only available legal basis for processing.** Controllers may now rely on a number of alternative grounds, including contractual necessity, legal obligations, publicly available data and protection of vital interests.
- **Automated processing and automated decision-making are now specifically regulated.** Individuals gain the right to object to decisions resulting from automated processing and organisations must ensure human review mechanisms are available.
- **Employment-related and security-related processing receive special treatment** through the introduction of new exemptions under Article 5 *bis*.
- **The definition of health data has been broadened**, potentially increasing the range of information that may be classified as sensitive data.
- **Data retention obligations have become stricter**, requiring deletion immediately once the purpose of processing has been fulfilled, subject to limited exceptions.

Recommended actions

Organisations that process personal data relating to individuals in Oman, whether from within Oman or abroad, should consider the following steps:

- Review whether the organisation is now within the territorial scope of the amended PDPL.
- Assess existing processing activities against the newly introduced legal bases for processing.
- Review HR, workforce management and CCTV processing activities in light of Article 5 bis.
- Reassess processing involving health, genetic or biometric data and determine whether any Ministry permit requirements continue to apply.
- Identify AI tools and other systems involving automated processing or automated decision-making.
- Establish procedures allowing individuals to challenge automated decisions and obtain meaningful human review.
- Update privacy notices and consent mechanisms to reflect the revised transparency requirements.
- Review retention schedules and deletion procedures.
- Reassess international transfers involving personal data relating to individuals in Oman.
- Monitor forthcoming guidance and Executive Regulation updates.

In depth

The PDPL now clearly reaches processing outside Oman

Perhaps the most significant change for international businesses is the new territorial scope. The PDPL now applies to the processing of personal data of natural persons “in the Sultanate of Oman”, whether that processing takes place inside or outside the country.

This means that a company may be subject to the PDPL even if it:

- Has no incorporated entity, branch or office in Oman
- Operates a regional or global platform from outside Oman
- Processes Omani customer, patient, user or employee data through an overseas group company
- Hosts Omani personal data in a global cloud environment
- Uses an overseas vendor to analyse or otherwise process data relating to individuals in Oman

Consent remains the default, but it is no longer the only route

The revised Article 10 continues to provide that personal data may not be processed, or used for a new purpose, without the data subject’s explicit consent. It also strengthens transparency around consent requests. These must be clear and understandable and must identify:

- The controller and any processor
- How the data protection officer can be contacted
- The purposes and nature of the processing
- Any other information required to meet the applicable processing conditions

Importantly, the Royal Decree introduces a new Article 10 bis, permitting processing without explicit consent where:

- The processing implements a legal obligation imposed on the controller under a law, judgment, order or court decision.
- The data is publicly available in a manner that is not contrary to the PDPL.
- The processing is necessary to protect a vital interest of the data subject and it is not possible to contact the individual.

- The processing is required to perform a contract to which the individual is a party, provided that the contract contains evidence that the processing will be conducted in accordance with the PDPL.

These new grounds are commercially important. Businesses may no longer need to rely on consent for certain standard processing activities, such as performing a customer contract or complying with a statutory obligation.

This brings the Omani framework closer to international best standards like GDPR, whose Article 6 also recognizes contractual necessity, legal obligations and vital interests as independent legal grounds. However, the alignment is incomplete. The Royal Decree does not introduce a general "legitimate interests" basis equivalent to Article 6(1)(f) GDPR, nor does it establish a broad public-task basis for private-sector controllers.

The contractual ground is also framed differently. The amended PDPL requires the contract to include evidence that personal data will be processed in accordance with the law. International companies should therefore not assume that a GDPR-compliant Article 6 assessment will automatically satisfy the Omani requirements.

Employee data and security cameras receive specific treatment and there are wider routes to process sensitive information

A new Article 5 bis allows a controller to process personal data in a number of operationally important scenarios, including:

- Processing the personal data of employees and other personnel where the processing is required with the controller's internal operations
- Processing is carried out through surveillance devices and cameras used to satisfy security requirements imposed by competent authorities
- Any additional cases that may be specified by the Minister

For employee-related processing, the exemption applies provided that the processing is carried out in accordance with the PDPL and the personal data is not disclosed to third parties without the data subject's written consent.

The significance of Article 5 bis lies in the fact that it is framed as an exception to Article 5 of the PDPL, which restricts the processing of certain sensitive categories of personal data, including health data, genetic data, biometric data, ethnic origin data, religious and political beliefs, and criminal records unless a permit is obtained from the Ministry.

This suggests that the new provision may provide greater flexibility for processing sensitive data in specific employment and security-related contexts. For example, employers may be able to rely on Article 5 bis when processing employee health data or other sensitive workforce information required for internal operations, while operators of security systems may benefit from a more streamlined basis for processing biometric or surveillance-related data.

That said, the extent of the exemption remains unclear because Article 5 itself has not been amended. Until further guidance is issued, organisations should continue to assess carefully whether any separate permit requirements remain applicable when processing sensitive categories of personal data.

A new rule for automated processing brings AI governance into focus

The Royal Decree introduces a broad definition of "automated processing". It covers processing conducted through an electronic program or system that operates either:

- Completely independently, without human involvement
- Partially automatically, with limited human supervision or involvement

This could capture a wide range of AI and algorithmic tools, including:

- Automated recruitment screening and candidate-ranking systems
- Tools used to assess creditworthiness or insurance risk
- Fraud detection and transaction-monitoring systems
- Healthcare triage, diagnostic-support and patient-prioritisation tools
- Employee performance and productivity tools
- Automated customer eligibility or account-suspension systems

- Generative AI applications that analyse, generate or infer information using personal data

Under revised Article 14, controllers and processors using automated processing must take appropriate measures to protect the privacy and confidentiality of personal data and prevent harm to data subjects. Individuals also have the right to object to decisions resulting from automated processing. When an objection is raised, the controller or processor must introduce a human element into the review of the decision, in accordance with controls to be set by the Executive Regulations.

This marks an important move towards the GDPR's approach to automated decision-making, but the two regimes are not identical. Article 22 GDPR generally gives individuals the right not to be subject to decisions based **solely** on automated processing where the decision produces legal or similarly significant effects, subject to specific exceptions. The amended PDPL appears broader in at least two respects:

1. Its definition includes partially automated processing with limited human involvement.
2. The right to object is not expressly limited to decisions producing legal or similarly significant effects.

At the same time, unlike the GDPR, the amended PDPL does not expressly require controllers to provide meaningful information about the logic involved in automated decision-making or its likely consequences. It also does not expressly set out exemptions for decisions that are necessary to perform a contract, authorized by law or based on explicit consent.

Pending further guidance, companies should take a cautious and risk-based approach to AI tools that make, influence or support decisions about individuals in Oman.

Health data is now defined more broadly

The Royal Decree expands the definition of "health data". It now covers personal data relating to an individual's physical, mental or psychological health condition, as well as data connected with the provision of healthcare services that reveals the person's health status.

The revised definition may therefore capture information that is not contained in a traditional medical record, including:

- Digital health and wellness information
- Information generated by connected medical devices
- Appointment, treatment and care-pathway information
- Health-related inferences produced by analytics or AI tools
- Information processed by telemedicine platforms
- Certain information relating to insurance claims or healthcare payments

Businesses should assess data according to what it reveals, rather than only by reference to where it came from. Data collected through a consumer-facing app, wearable or customer service interaction may constitute health data if it reveals an individual's health condition.

Data must generally be deleted as soon as its purpose ends

The amended Article 15 requires controllers and processors to erase personal data immediately once the processing purpose has ended. Retention is permitted only where:

- There is an existing dispute between the controller or processor and the data subject.
- Retention is needed to comply with a legal obligation arising under a law, judgment, order or court decision.

Businesses should not assume that global corporate retention schedules will automatically work for Oman. In particular, retention based only on internal policy, business convenience or a generalized risk-management rationale may be difficult to justify unless it falls within an applicable legal obligation or relates to an existing dispute.

Looking ahead

The amendments represent an important evolution of Oman's privacy landscape. By expanding the law's territorial reach, introducing additional legal bases for processing and establishing specific safeguards around automated processing, Oman is moving towards a more mature and internationally recognisable privacy framework.

At the same time, important questions remain, particularly regarding the interaction between the new Article 5 bis exemptions and the existing permit requirements for sensitive personal data. Organisations should therefore continue to monitor further guidance from the Ministry of Transport, Communications and Information Technology and any subsequent amendments to the Executive Regulations.

Contact Us

Dino Wilkinson
Partner
dino.wilkinson
@bakermckenzie.com

Lucrezia Lorenzini
Senior Associate
lucrezia.lorenzini
@bakermckenzie.com