

Data privacy handbook for the Sultanate of Oman

**A starter guide to compliance with
the Personal Data Protection Law of
the Sultanate of Oman**



pwc



Contents

01

A quick introduction to data privacy



02

About this handbook



03

Why is data privacy important?



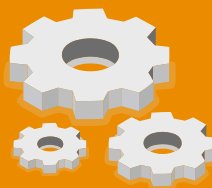
04

Key concepts



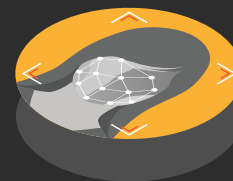
05

Key principles of data privacy



06

What is personal data?



07

What is sensitive personal data?



08

Controllers vs processors



09

Personal data owner's rights



10

When can personal data be processed?



11

Ten steps to an effective data privacy programme



12

How PwC can help



A quick introduction to data privacy

There are many definitions for “data privacy”. The simplest way to think about it is that people (customers, employees, anybody!) need to know what personal data organisations are collecting about them and how they are using it. Of course, this is a simplistic way to look at the topic but it is useful to set the scene.

Data privacy is far more than just the security and protection of personal data. It all boils down to how organisations are using that personal data. Organisations need to process personal data in an ethical and legal manner. That could mean not bombarding customers with unwanted SMS marketing messages but it could also mean simply not sharing personal information with third parties without the customer’s consent. It doesn’t mean that marketing is now forbidden under the Omani Personal Data Protection Law but it does mean that organisations need to be transparent about what personal data they are capturing and how it’s going to be used. Many organisations recognise the significant risks of cyberattacks and data breaches but fail to understand what else is required under the Omani Personal Data Protection Law.





In the past year there were series of high-profile data breaches followed by mega-fines from regulators. This has increased awareness about the importance of data privacy and protection. In February 2022 the Sultanate of Oman issued the Personal Data Protection Law, which set stricter standards for data privacy and protection and further increased awareness around the importance of data protection compliance.

In the Middle East some GCC states have already adopted their own privacy laws and other states have signalled their intent to release similar legislation in the near future. Many of the recent data privacy laws, including local Middle East data protection laws, have striking similarities with the General Data Protection Regulation (“GDPR”) - the main data protection law in the European Union. This is not surprising because the GDPR radically overhauled data privacy practices and is now considered the gold standard in data privacy worldwide.



About this handbook

The data privacy landscape is complex and it continues to evolve. It presents many challenges to organisations by creating uncertainty on many levels about whether, how, and when to process personal data. The adoption of the Omani Personal Data Protection Law means that there will be a significant impact on entities operating within the Sultanate of Oman. **The law comes into force on 13 February 2023 – and it is highly important for organisations to fully prepare themselves for compliance with the new legal requirements by this date.**

We've put together this Data Privacy Handbook for the Sultanate of Oman to try to simplify the requirements and help you to kick-start your data privacy compliance journey.

This toolkit reflects the requirements of the Omani Personal Data Protection Law, as well as some useful steps to ensure compliance with the law. The toolkit is suitable for all organisations processing personal data and looking for a practical approach to build their data privacy programmes. It's worth also noting that the Omani Personal Data Protection Law refers to "Executive Regulations" which will be issued later by the Minister of Transport, Communications and Information Technology. These Executive Regulations will give additional details about how organisations should comply with the law. After the Executive Regulations are issued, we will update this handbook accordingly.

Why is data privacy important?

Companies that fail to protect personal data and comply with data privacy regulations aren't just risking financial penalties. They also risk operational inefficiencies, intervention by regulators and - most importantly - permanent loss of consumer trust.

Regulatory

The regulator may order to erase the personal data that was processed not in compliance with the law or even order suspension of processing personal data.

Reputational

Non-compliance with the law could result in brand damage, loss of consumer trust, loss of employees' trust and customer attrition.



Financial and criminal

The Omani Personal Data Protection Law provides for high fines of up to **OMR 500,000** (around USD 1.3 mln). Violation of privacy may also be punished in some cases by **imprisonment of up to 1 year** (under the Omani Penal Law). You may also experience loss of revenue and high litigation and remediation costs.

Operational

Most data privacy laws give people more rights over their data, such as the right to access their data or the right for it to be deleted. This can be a significant operational burden if it is not implemented effectively.

Key concepts

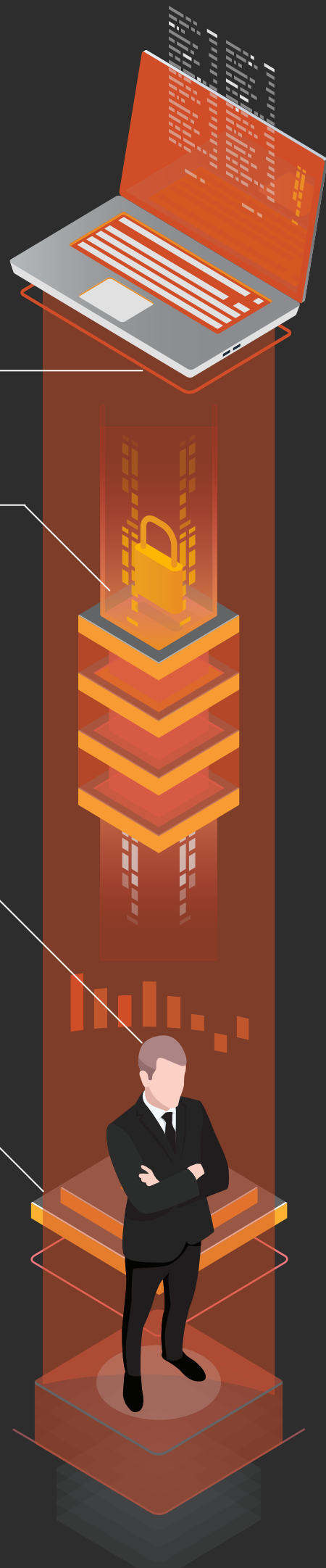
The Omani Personal Data Protection Law introduces a number of new terms and concepts which are important for you to familiarise yourself with, before continuing.

“**Personal Data**” means data that makes it possible to identify a natural person, either directly or indirectly. *Please refer to page 10 for further details.*

“**Data processing**” or “**Processing**” means any automated or manual operation(s) on personal data. In essence, this covers almost any action that could possibly be performed on personal data including collecting, recording, analysing, organising, storing, modifying, amending, retrieving, revising, coordinating, combining with each other, blocking, erasing or disclosing such data by sending, disseminating, transferring or making it available to other persons by any other means.

“**Personal Data Owner**” means any person who may be identified with the use of this person’s personal data.

The key Omani regulatory authority in the area of personal data is the **Ministry of Transport, Communication and Information Technology of the Sultanate of Oman** (hereinafter, the “Ministry”).



Key principles of data privacy

Most data protection laws are built on a set of key principles, which establish the foundation for everything related to data privacy and the protection of personal data. For instance, pursuant to the Omani Personal Data Protection Law, the personal data may only be processed within the framework of principles of **transparency, fairness and respect of human dignity**. In essence, it should mean that you must always process personal data strictly in accordance with the applicable legal requirements, acting in a fair and transparent manner with the personal data owners and regulators. You must also ensure that processing of personal data (as such) must not lead to negative consequences for the personal data owner.

It is also worth mentioning additional six important principles. They are not expressly listed in the Omani Personal Data Protection Law, but they will help you to ensure overall compliance with this law and to be in alignment with international data protection best practices.

The principles are:

Purpose limitation

You should only process personal data for a specified and lawful purpose.

Data minimisation

You must ensure you are only processing the personal data which you truly need and nothing more.

Accuracy

You should ensure personal data is kept up to date, and that necessary measures are in place for correcting and updating inaccurate data.

Storage limitation

You must not keep personal data for longer than you need it.

Integrity and confidentiality

You must implement adequate security controls to ensure that personal data is protected against loss, destruction or damage.

Accountability

You must have appropriate measures and records in place to be able to demonstrate your compliance.



What is personal data?

Personal data is any information that can identify a natural person. This could be as simple as a name or account number or could be a digital identifier such as IP address, username or location data such as GPS coordinates.



It's important to be aware that an individual can be identified either:

- Directly, if you are able to identify a specific individual solely through the data you're processing. Examples: name, ID number, email address.
- Indirectly, if different sets of data from different sources, when combined, could identify a specific person. Examples: gender, birth date, licence plate number.

What is sensitive personal data?

Some personal data is considered sensitive, as it could cause significant harm to the individual if leaked or misused. Processing of such personal data is often subject to extra restrictions.

The Omani Personal Data Protection Law provides for additional protection of the following personal data:

- »» Genetic data (e.g. results of analysis of biological samples)
- »» Biometric data (e.g. facial images)
- »» Health data
- »» Ethnic origin
- »» Sex life
- »» Political or religious opinions and beliefs
- »» Criminal convictions
- »» Security measures



Processing of the above data is allowed only upon obtaining a permit from the Ministry. The Executive Regulations will specify controls and procedures relevant to processing such sensitive personal data.

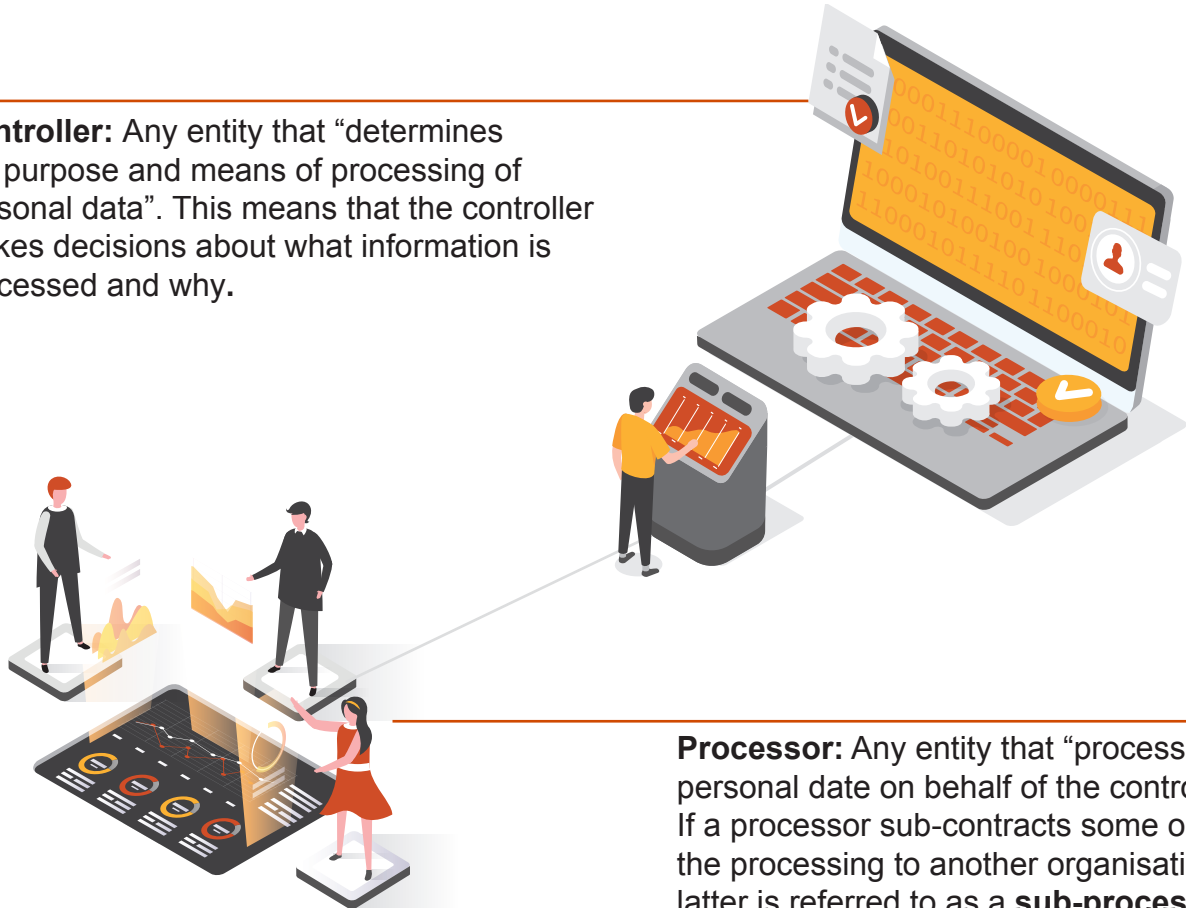
Processing of sensitive personal data in violation of the Omani Personal Data Protection Law may be punished with a fine up to **OMR 20,000** (around USD 50,000) and in some cases with a fine up to **OMR 100,000** (around USD 260,000). Depending on the circumstances of the case, misuse of such personal data may even lead to criminal liability in the form of **imprisonment** (under the Omani Penal Code). The court may also order **confiscation** of processing equipment.



Controllers vs processors

The Omani Personal Data Protection Law draws a clear distinction between the “Controller” and the “Processor” to recognise that not all organisations involved with the processing of personal data have the same responsibilities.

Controller: Any entity that “determines the purpose and means of processing of personal data”. This means that the controller makes decisions about what information is processed and why.



Processor: Any entity that “processes personal data on behalf of the controller”. If a processor sub-contracts some or all of the processing to another organisation, the latter is referred to as a **sub-processor**.

A simple way to think about this is as follows. A retailer creates an e-commerce website and decides what information it requires from customers to create an account. The retailer uses a cloud provider to host their website and database. In this case, the retailer is the data controller and the cloud provider is the data processor.

Am I a controller or a processor?

It is important to note that an organisation is not by its nature always acts as either a controller or a processor. It may be acting as a controller for some personal data processing activities, and as a processor – for others.

Therefore, the organisation must understand whether or not it determines the purposes and means of processing of personal data. If it determines such purposes and means – the organisation is a controller. If the organisation only processes personal data under the instruction of another entity – such an organisation is likely to be a processor.

What does it mean if I am a..



Controller

You are ultimately accountable for your own compliance and the compliance of your processors. Your responsibilities include compliance with the Omani Personal Data Protection Law, including compliance with data protection principles, responding to individuals' rights, enforcing security measures, managing data breaches and engaging only those processors that are capable of protecting the data effectively.

Processor

You have less autonomy over the data you're processing, but you may still have direct legal obligations. If you engage a sub-processor, you may be liable to the controller for the sub-processor's compliance.

Your responsibilities include compliance with your controllers' instructions as could be given under the contracts concluded with the controller, enforcing security measures and notifying controllers of personal data breaches.



Sub-processor

As a sub-processor, you may be liable for any damage caused by your processing in case you have not complied with your legal obligations and if you failed to follow the instructions from your counterparty. Your responsibilities towards the processor are similar to the processor's responsibilities towards the controller.



Personal data owner's rights

One of the aims of data privacy laws is to empower individuals and give them control over their personal data. The Omani Personal Data Protection Law also provides individuals with a number of rights for the purpose of better protection of their interests in the area of data protection. It's important to note that not all of these rights are "absolute", meaning some only apply in specific circumstances:

Right to withdraw consent to data processing

Individuals have the right to withdraw consent that they earlier gave for the purpose of data processing.

Right to request correction, updating or blocking of personal data

Individuals can have their personal data rectified if their data is inaccurate, or completed if such data is incomplete.

Right to transfer personal data

Individuals may request transfer of personal data to another controller.

Right to obtain a copy of the personal data being processed

Individuals have the right to request copies of their personal data.

Right to be notified of a data breach

Individuals shall be notified of incidents that involve breach of their personal data.

Right to request erasure of personal data*

Individuals may request erasure (deletion) of their personal data.



* As mentioned above, not all rights are "absolute". The "right to erasure" is often misunderstood. The main reason for this is because many assume that it is an "absolute right", whereas in fact there are only certain circumstances when people can request for their data to be deleted. For example, the public authority may be required to keep records with your personal data for some time and your right to request erasure may potentially not be applicable here.

When can personal data be processed?

As a general rule, the Omani Personal Data Protection Law allows to process personal data only upon obtaining in writing explicit consent of the personal data owner.

However, the law provides for a number of **exceptions, when its provisions (including the requirement to the written explicit consent) shall not apply**. Such exceptions include:

Protection of national security or public interest.

Execution by units of administrative apparatus of public legal entities of their powers, as they are prescribed to them by the law.

Performance of a legal obligation imposed on 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 personal data owner.

Detection or prevention of any criminal offense based on an official written request from the investigation authorities.

Performance of a contract to which the personal data owner is a party.

If processing is in a personal or family context.

If processing is for the purposes of historical, statistical, scientific, literature or economic research (under certain conditions).

If the data is publicly available and such availability does not violate provisions of the Omani Personal Data Protection Law.

Top tips

- Carefully assess if your processing may fall under any exceptions, as specified in the Omani Personal Data Protection Law. If not – ensure you obtain documented explicit consent from the personal data owner.
- If you intend to process any sensitive personal data (as listed on page 11 of this handbook) – seek approval from the Ministry and ensure compliance with additional requirements of the Executive Regulations (where applicable).

Ten steps to an effective data privacy programme



1

Appoint a data protection officer

18

2

Maintain a personal data register

19



Notify purpose and seek consent

3

20

4

Respond when individuals ask about their personal data

21



Enforce security mechanisms

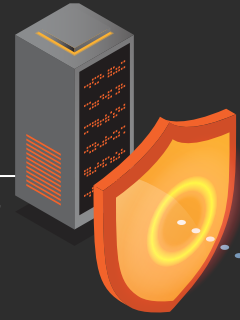
5

22

6

Embed data privacy into your systems, processes and services

24



Notify data breaches

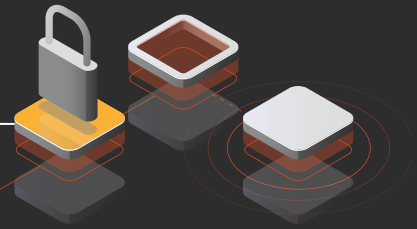
7

26

8

Manage contractors

27



Protect personal data when transferring outside the Sultanate of Oman

9

28

10

Communicate your data protection policies, practices and processes

29



1 Appoint a data protection officer

Many data privacy laws introduce the concept of a "Data Protection Officer" ("DPO"), a new leadership role for overseeing the organisation's data protection programme and ensuring compliance with the applicable laws. The Omani Personal Data Protection Law expressly requires controllers to appoint a DPO. It is expected that the Executive Regulations will provide more details on the appointment of DPO and DPO's duties.

Who could act as a DPO?

You can assign the role of DPO to an existing employee within your organisation, or recruit someone specifically for this role.

The DPO must be independent, an expert in data protection, adequately resourced, and must report to the highest management level.

What's the role of a DPO?

The DPO assists you in monitoring internal compliance with the applicable data protection laws, advising you on your data protection obligations, providing expert advice when needed, and acting as a point of contact for individuals and data protection authorities.



2 Maintain a personal data register

In order to protect personal data you need to know what data you collect, how you use it and where you store it. The first step in achieving this is identifying all processing activities in your organisation involving personal data, and documenting how and why the data is used in what is called “Record of Processing Activities”.

How can I identify personal data being processed?

Maintaining a personal data register is one of the key requirements of most data privacy regulations worldwide. The Omani Personal Data Protection Law does not expressly require to maintain such a register. However it requires to keep the documents related to the processing operations (in accordance with the timelines and procedures determined in the Executive Regulations). Therefore, in order to fulfil this requirement and to achieve effective compliance with the Omani Personal Data Protection Law it is highly important to maintain a personal data register. As a first step, we recommend that you undertake a data discovery exercise across your organisation to document what personal data you hold and process, where it’s located, who has access to it and how long it is retained.

What details should I include in the register?

It is recommendable to identify and document at least the following for every processing activity within your organisation:

- Name and contact details of your DPO
- Purpose of processing the data
- Categories of personal data involved
- Systems and locations where the personal data is processed
- Where the data is transferred to and the list of recipients
- Retention period and enforced technical and security measures
(Please refer to page 22 for more details)



3 Notify purpose and seek consent

The Omani Personal Data Protection Law requires organisations to be transparent about how they use personal data. When collecting personal data from individuals, you must provide them with clear and sufficient information explaining what, why and how you're intending to process.

What information should I provide?

At least the following information must be included into the privacy notice to be shared with individuals:

- Details of the controller and the processor.
- Contact details of the data protection officer.
- Purpose of processing of the personal data, as well as the source from which the data was collected.
- Full and accurate description of the processing and its procedures, as well as the extent of disclosure of personal data.
- Rights of the personal data owner, including the right to access, to correct, to transfer, and to update the personal data.
- Any other information that may be necessary to fulfill the conditions of processing.

When to provide it?

The above information must be provided to personal data owners before the start of processing of their personal data.

How to provide it?

Privacy information must be concise, transparent, intelligible, easily accessible and with the use of clear and plain language. To meet these requirements, you could consider using a combination of techniques, such as an expandable section approach, dashboards and just-in-time notices.

What is consent?

Consent may be defined as a freely given, specific, informed and unambiguous agreement, provided by individuals through a statement or a clear affirmative action, to the processing of their personal data.

Consent means giving people control and choice over how their personal data is processed. It constitutes the key legal ground for lawfully processing personal data under the Omani Personal Data Protection Law.

How can I obtain consent?

- Under the the Omani Personal Data Protection Law the consent must be obtained at the controller's request which shall be in writing, in a clear, explicit and understandable manner.
- Consent must be given by individuals in writing. It should be distinct from any other agreement (e.g. terms and conditions) and expressed using clear and simple language.
- Individuals can rightfully withdraw their consent at anytime, and the withdrawal procedures should be as easy as those for giving the consent.
- Processing of personal data of a child is allowed only after obtaining consent of the child's guardian, unless such processing is in the best interest of the child (this kind of processing will also need to meet requirements of the Executive Regulations).



4 Respond when individuals ask about their personal data

What are personal data owners' requests?

The Omani Personal Data Protection Law introduces new rights for individuals that are designed to give them more control over their data. Individuals are entitled to raise requests to exercise their data rights (e.g. to request a copy of their data, to request erasure of their data, etc.) and organisations must respond to their requests.

How can I be prepared?

To meet the defined timeline, your organisation has to implement robust procedures to authenticate the requester, assess the request and formulate an adequate response.

What information should I provide in my response?

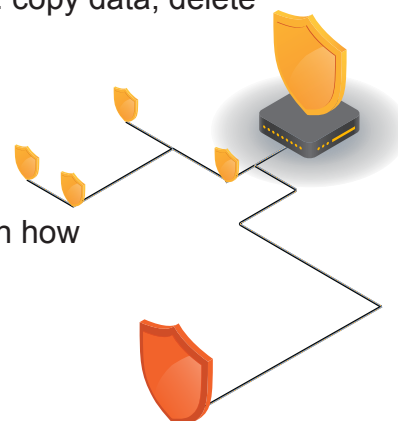
The Omani Personal Data Protection Law does not expressly say what information must be specified in the response to the request of the personal data owner. Such information will depend on a particular request. That said, the following information is likely to be specified in the responses in most of the cases:

- What personal data is being processed. Please refer to page 10 for further details.
- Purpose and legal ground for processing the personal data.
- Who within the organisation has the personal data and who it will be disclosed to.
- How long the data will be retained for, or at least the criteria used to determine this period.

What are the steps to responding to the request?

1. Receive the personal data owner's request and forward it to the concerned department.
2. Determine if the request is self-raised or on behalf of others, then verify the identity of the individual.
3. Assess the request and confirm if it based on the law and if any specific requirements apply to it.
4. Determine where the personal data of the individual is stored, be it in systems or physical documents.
5. Perform the appropriate action according to the type of the request (i.e. copy data, delete data, restrict processing, etc).
6. Provide appropriate details to the DPO for response to the request.
7. Send and document the appropriate response to the individual.

It is expected that the Executive Regulations will provide more guidance on how to respond to the requests of the personal data owners.



5 Enforce security mechanisms

The Omani Personal Data Protection Law requires the controller to ensure confidentiality of the personal data being processed. For this purpose the organisations must take appropriate organisational and technical measures. Specific measures shall depend on the organisation's size and the amount and type of personal data being processed.

Generally speaking, organisational and technical measures are the functions, processes, controls, systems, procedures and measures taken to protect and secure the personal data that you process.

Organisational measures could be defined as the approach taken in assessing, developing and implementing controls that secure information and protect personal data. They can include, but are not limited to:

- Policies and procedures
- Business continuity
- Risk assessments and audits
- Awareness and training

Technical measures could be defined as the measures and controls implemented on systems from the technological perspective. Such measures go beyond securing access to devices and systems. They can include, but are not limited to:

- System and physical security
- Encryption or de-identification (anonymisation) of personal data
- Robust data disposal measures
- Passwords and two-factor authentication
- Securely and reliably implemented technologies, such as bring your own device (BYOD) and remote access



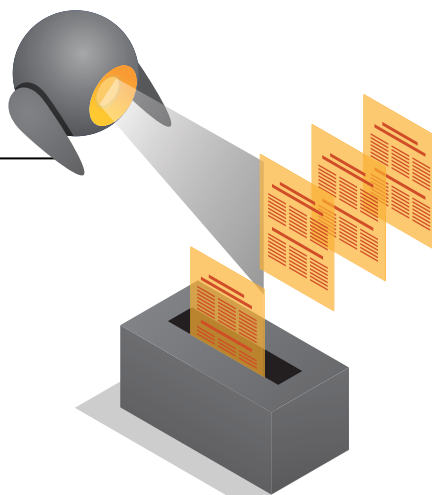
Which security measures should I implement?

Depending on the size of your organisation and the processing activities undertaken, there are a broad range of technical and organisational measures that can aid in securing and protecting personal data. We also suggest utilising established frameworks such as ISO27001 to assess and develop adequate measures.

As there is no “one size fits all” solution when it comes to information security, we recommend you following the steps below to determine which measures you should implement:

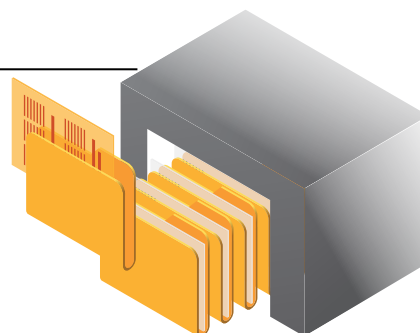
Step 1

Carry out an information security risk assessment by reviewing the personal data you hold, the way you use it, and the risks presented by the processing.



Step 2

Carry out a technical vulnerability assessments (e.g. a penetration test) on devices and systems posing high risk on your personal data processing.



Step 3

Assess and select the most adequate security measures to mitigate the identified risks.



Step 4

Ensure your employees are kept up to date on your information security programme and latest security best practices.



6 Embed data privacy into your systems, processes and services

The Omani Personal Data Protection Law requires the controller to implement technical and procedural measures to ensure that the processing is carried out in accordance with the law. This is similar to the internationally recognised concepts of data privacy by design and data privacy by default. A first step to translate these broad concepts into functional requirements is to define their key principles as follows:

1. Privacy and data protection are embedded into the design of a new process or application (example: application does not disclose to anyone the personal data of the smartphone owner, unless such a disclosure is authorised by the owner).

2. Transparency is created and maintained (example: privacy notices are regularly updated to reflect the processing activities and privacy practices).

3. Safeguards are established and enabled (example: enforcing encryption and data minimisation mechanisms on personal data).

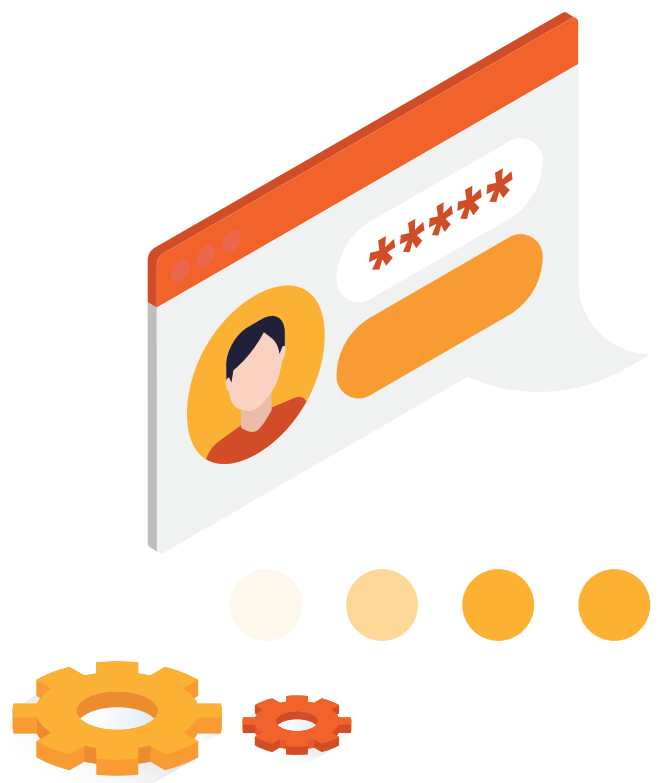
While these principles help to inform the organisation's overall approach, successful privacy by design and default is facilitated by governance and oversight, implemented by a supportive workforce, and informed by risk and compliance.

What is “data privacy by default”?

Data privacy by default links to the fundamental data protection principles of data minimisation and purpose limitation.

Privacy by default requires you to ensure that you only process personal data that is necessary to achieve your specific purpose, while considering things like:

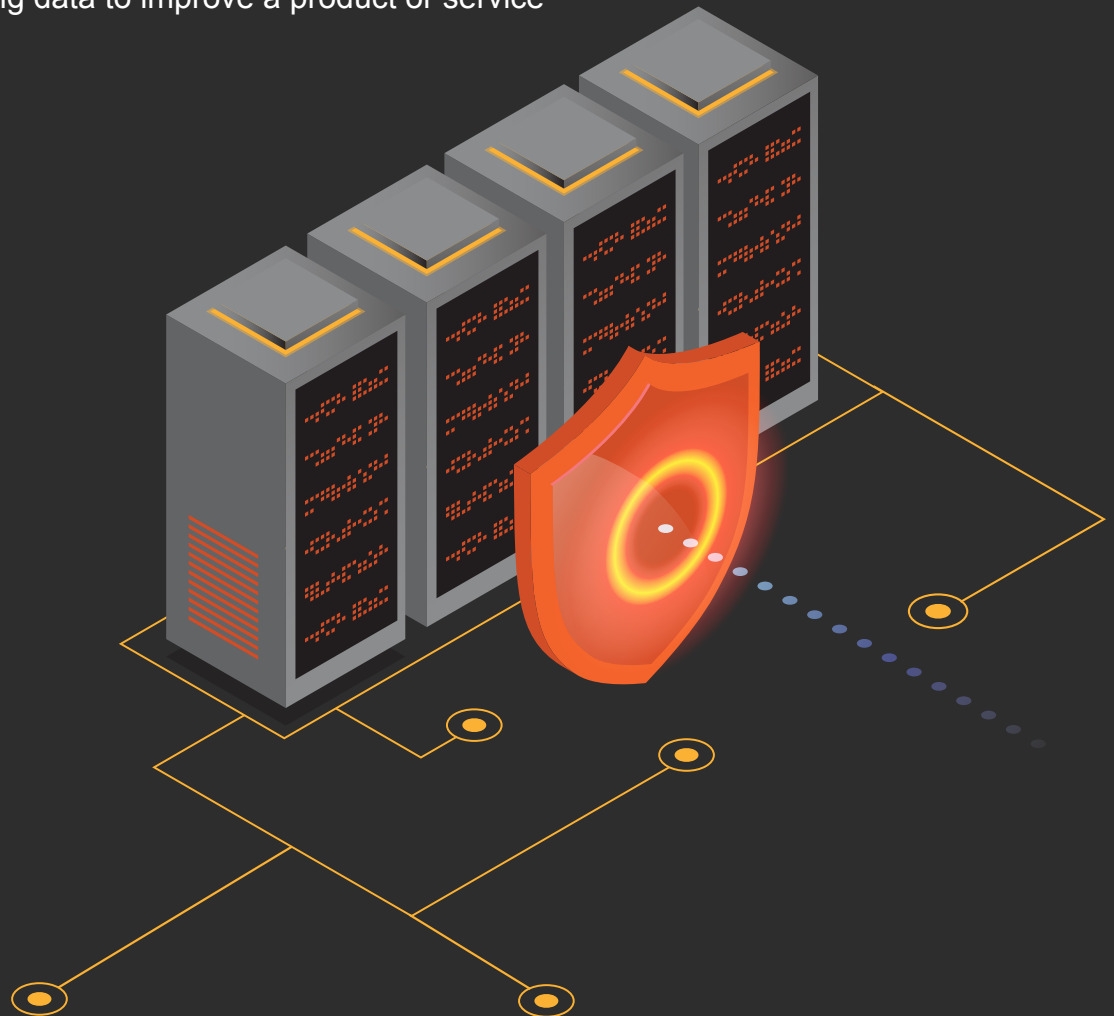
- adopting default privacy settings on systems
- being transparent about your data processing activities
- providing information and options to individuals to exercise their rights



What is “data privacy by design”?

Data privacy must be embedded into the design and overall lifecycle of any technology, business process, product, or service, such as:

- Using a new way for storing data (i.e. cloud)
- Engaging a contractor to manage and maintain an IT system
- New or changing business process
- New product offering
- New use of existing data to improve a product or service



Privacy by design requires you to:

- Put in place appropriate technical and organisational measures to implement the data privacy principles; and
- Embed controls into your processing activities so that you protect individuals' rights.

Privacy by design is mainly comprised of two distinct elements:

1. Data Privacy Impact Assessment (“DPIA”): a tool used to identify and manage data privacy risks.
2. Personal Data Change Management: a process which governs how changes to business processes or applications are managed.

7 Notify data breaches

Data breaches can happen for various reasons, despite all the precautions that you may take. Pursuant to the Omani Personal Data Protection Law the controller shall notify the Ministry and the personal data owners of the occurred breach. Specific procedures on notifying the data breach will be determined in the Executive Regulations.

Below we outline some practical steps that may be considered in the event of a data breach.

How do I respond to a data breach?

Once a breach is discovered:

- Assess the nature of the breach and confirm if personal data is involved.
- Identify what personal data has been impacted and how.
- Assess the risks to the rights and interests of individuals.
- Carry out a thorough investigation to identify the source of the breach and take necessary remediation actions.



Notifying affected individuals

You need to notify them at least of the breach's nature, consequences and measures taken to address it.

Notifying the Authority

Your breach notification should include the following information at a minimum:



- Nature of breach:
 - Who accessed what and when?
 - What caused the breach?
 - How was the data used?
 - Who are the affected individuals?
- Description of the estimated impact and possible effects.
- Contact details of your data protection officer.
- Measures taken by you to investigate and remediate the breach.

Top tips to beat the clock

- Ensure that your systems can detect the data breach as early as possible.
- Stay calm and take the time to investigate thoroughly before getting your business back up and running.
- Put a response plan in place and communicate it to all employees and contractors (where applicable).
- Regularly test the plan to minimise the disruption that typically follows a breach.
- Allocate the responsibility for managing breaches to a dedicated person or team.

8

Manage contractors

The Omani Personal Data Protection Law requires the controller to ensure that the processing is performed in compliance with the law. Therefore, if you engage contractors to process personal data (processors), you may be held liable if your contractor violates applicable requirements of the Omani Personal Data Protection Law while providing the services to you.

When entering into an agreement with your contractor, ensure there are clauses that require the contractor to take sufficient measures to ensure compliance with the requirements of the law.

What should I include in a contract?

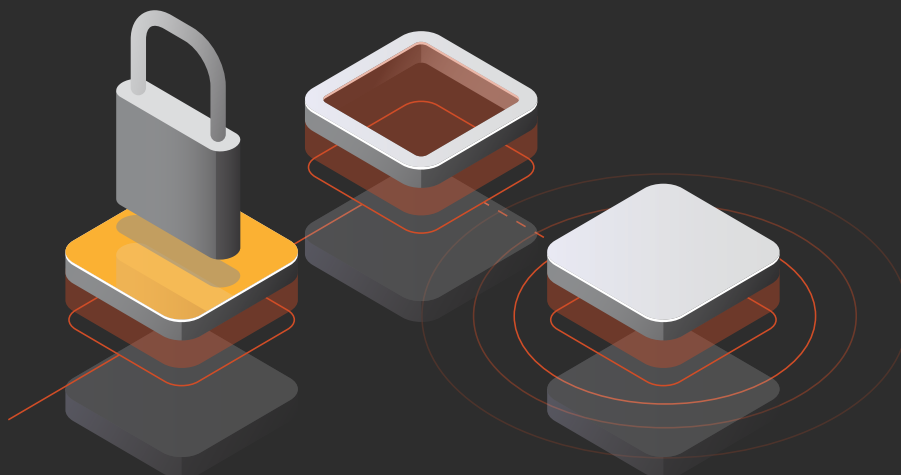
Contract with the processor shall at a minimum include the following details:

- Subject-matter and duration of processing.
- Nature and purpose of processing.
- Types of personal data and categories of personal data owners.
- Obligations and rights of the parties.
- Timelines of the processing.
- Liability of the parties.
- Controller's right to conduct an audit on the processor (to assess its compliance with the contract and with the law).

Enhancing your risk management programme related to contractors

Contracts alone are not enough to manage risks associated with engaging contractors. We outlined below examples of additional steps you can consider to enhance your risk management programme:

- Conduct a due diligence assessment to ensure that the contractor has adequate controls in place to protect personal data.
- Update your existing contracts and draft new contracts clearly defining the roles, responsibilities and liabilities of both parties.
- Continue to improve ongoing monitoring through risk assessments and audits to ensure that contractors are maintaining adequate controls to protect personal data.



9 Protect personal data when transferring outside the Sultanate of Oman

The Omani Personal Data Protection Law generally **allows the controller to arrange transfer of personal data outside the Sultanate of Oman (cross-border transfer)** - subject to compliance with the requirements and restrictions that shall be specified in the Executive Regulations.

The law prohibits to transfer personal data abroad if it was processed in violation of the law, or if it would cause harm to the personal data owner (it remains to be seen how the latter restriction will be interpreted in practice).

What is considered a cross-border data transfer?

- You are making a cross-border data transfer if you send personal data to a receiver that is located outside the Sultanate of Oman.
- Please note that:
 - Restrictions on cross-border transfer will apply also if the personal data is transferred within the same corporate group (if the sender and receiver are entities that are located in different countries).
 - Restrictions are also likely to apply if the personal data remains in the Sultanate of Oman, but the access to it is given to someone located outside the country.



10 Communicate your data protection policies, practices and processes

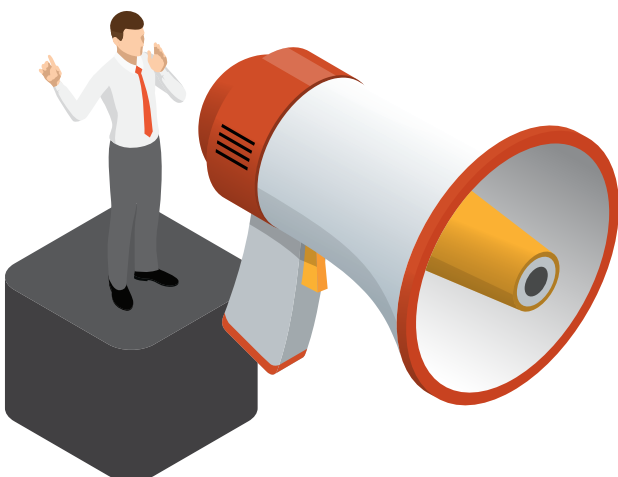
Complying with data privacy laws is not something that can be left to the legal and compliance departments alone. Compliance with data privacy laws requires that everybody in the organisation understands their responsibilities to protect personal data. It is very important to communicate your data privacy policies and practices to your **customers** and **employees** to ensure they are familiar with how you process and protect personal data.

Customers

- Make the business contact information of your data protection officer easily accessible so that your customers know who to contact for inquiries or complaints.
- Readily provide information about your data protection policies, practices and complaints process upon request.
- Update your privacy notice to make sure your customers understand what personal data you process, and how you do it, to enable them to make informed decisions about it. The privacy notice should be:
 - Concise and transparent
 - Written in clear and plain language
 - Delivered in a timely manner
 - Made publicly available and easy to access






Employees

- Communicate your data protection policies and practices to your employees, to make sure they are familiar with their roles and responsibilities in processing personal data.
- Develop a culture of privacy awareness within your organisation by aligning the importance of data privacy to your values and implementing practical approaches to convert it to repeated practices.
- Use posters, email and other communication tools to raise awareness of the importance of personal data protection among your staff.
- Send key employees who handle personal data to attend regular data privacy training to ensure they are kept up to date on your internal processes and latest developments in the privacy area.



How PwC can help

As experts in data privacy, we are well positioned to support you with your organisation’s journey to data privacy compliance. We have developed a five step approach to transforming privacy programmes, with tools and accelerators to assist the process.

Assess current capabilities	Data discovery	What you will get <ul style="list-style-type: none"> • Stakeholder engagement and communications plan • Personal data inventory • Data flow maps showing the movement of personal data from collection through to disposal 	
	Gap assessment	What you will get <ul style="list-style-type: none"> • Control gap analysis • Risk assessment based on current and planned future uses of personal data 	
Design the future state	Target operating model and programme design	What you will get <ul style="list-style-type: none"> • Detailed remediation project plan with identified organisational impact • Cross-functional working group established 	
	Programme implementation	Areas of focus <ul style="list-style-type: none"> • Strategy and governance • Policy management • Cross-border data strategy • Data life-cycle management • Individual rights processing • Privacy by design • Information security • Privacy incident management • Data processor accountability • Training and awareness 	
Operate and sustain	Ongoing operations and monitoring	What you will get <ul style="list-style-type: none"> • Defined ongoing monitoring programme • Tracking and retesting of non-compliance • Protocols for changes to policies and procedures 	

Get in touch

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



Omar Al Sharif
Oman Country Senior Partner
+968 2455 9118
omar.al-sharif@pwc.com
linkedin.com/in/omar-al-sharif-7421024/



Matthew White
Partner, Digital Trust Leader
+971 56 113 4205
matthew.white@pwc.com
linkedin.com/in/mjwme



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



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



Nakul Srivastava
Director, Digital Trust
+974 50 692 483
nakul.srivastava@pwc.com
linkedin.com/in/nakul-srivastava/



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



At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 156 countries with over 295,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

Established in the Middle East for 40 years, PwC has 22 offices across 12 countries in the region with around 7,000 people. (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.