Data privacy handbook for the Kingdom of Saudi Arabia

A starter guide to compliance with the Saudi Arabia Personal Data Protection Law

Version 2

September 2023

pwc

Contents

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 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. Organisations need to process personal data in an ethical and legal manner. That could mean not bombarding individuals with unwanted SMS marketing messages but it could also mean simply not sharing personal data with third parties without the necessary controls or safeguards. It does not mean that marketing is now forbidden under the Saudi Personal Data Protection Law (“**PDPL**”) but it does mean that organisations need to be transparent about what personal data they are capturing and how it is going to be used. Many organisations recognise the significant risks of cyber attacks and data breaches but fail to understand what else is required under the PDPL.

In the past years there were series of high-profile data breaches followed by mega-fines from regulators in various regions. This has increased awareness about the importance of data privacy. In September 2021 the authorities of Saudi Arabia issued the PDPL, which set stricter standards for data privacy and protection and further increased awareness around the importance of data protection compliance. In March 2023 the updates to the PDPL were adopted and in April 2023 the updated PDPL was published.

The PDPL came into force on 14 September 2023. However it will become fully enforceable starting from 14 September 2024. Until this date the organisations have time (grace period) to take necessary steps to achieve their compliance with the new legal requirements.

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 introduction of the PDPL means that there will be a significant impact on organisations which operate in or do business with Saudi Arabia because they will need to develop data privacy programmes to meet the requirements of the law.

We have prepared this data privacy handbook for Saudi Arabia to try to simplify the legal requirements and to help you to kick-start your data privacy compliance journey.

This handbook reflects the requirements of the PDPL and PwC's own data privacy frameworks. The handbook is suitable for all organisations processing personal data and provides a practical approach to how organisations can build their data privacy programmes. It is worth also noting that PDPL mentions "Implementing Regulations" which were issued in September 2023. These Implementing Regulations provide for more details on how organisations should comply with the PDPL. We will identify where the Implementing Regulations impact our guidelines and we will update this handbook accordingly.

Why is data privacy important?

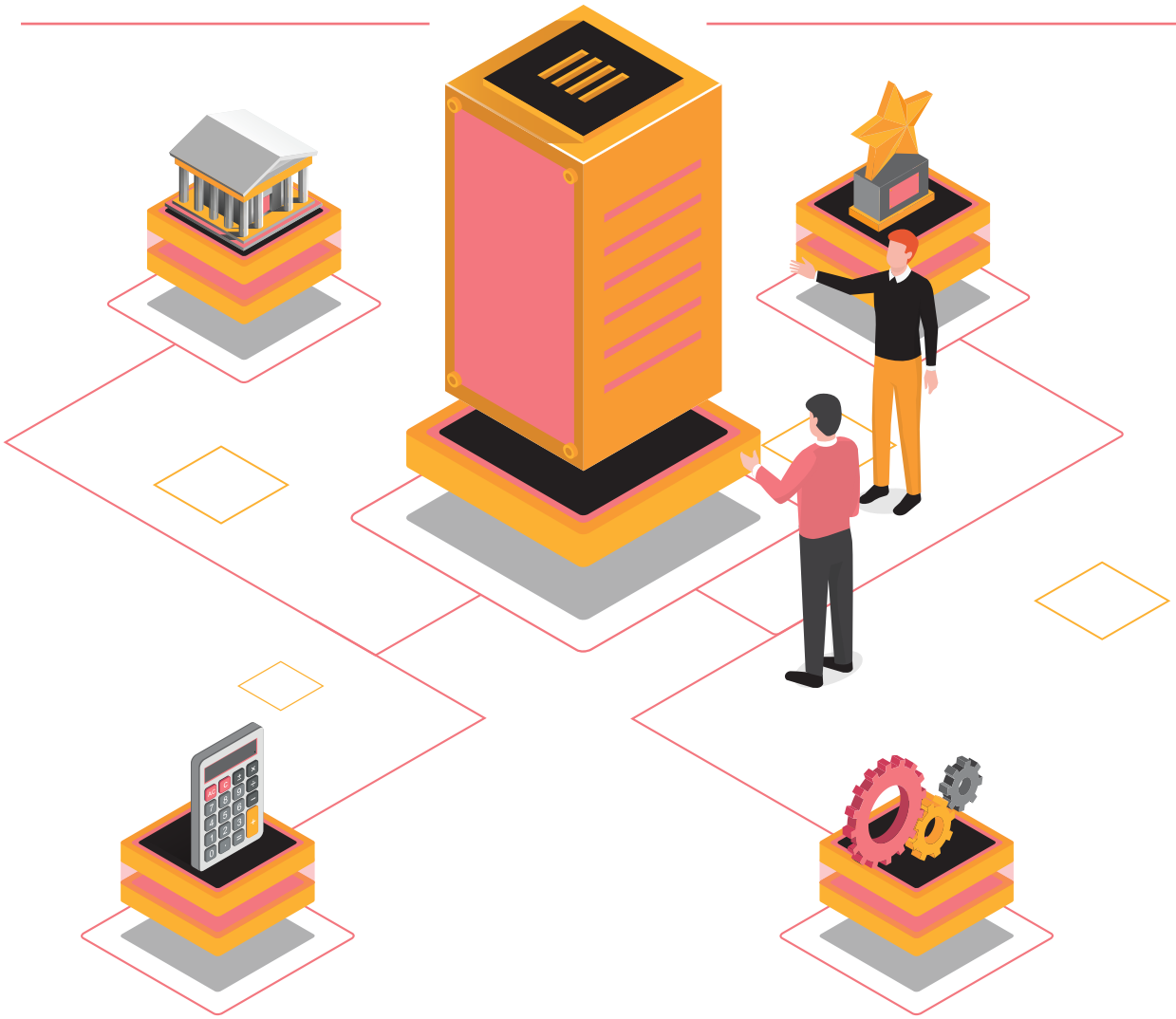
Companies that fail to protect personal data and comply with data privacy regulations are not just risking financial penalties. They also risk operational inefficiencies, intervention by regulators and - most importantly - permanent loss of consumer trust.

Regulatory

Data protection regulators may enforce mandatory audits, request access to documentation or even order that an organisation stops processing personal data.

Reputational

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



Financial and criminal

For data privacy violations the PDPL provides for fines of up to **SAR 5 million** (around USD 1.3 million) and **up to 2 years in prison**.You may also experience loss of revenue and high litigation and remediation costs.

Operational

The PDPL provides for certain rights to individuals over their personal data, such as the right to access their personal data, the right to request its deletion, etc. This can be a significant operational burden if it is not implemented effectively.

Key concepts

The PDPL introduces a number of new terms and concepts which are important for you to familiarise yourself with, before continuing.

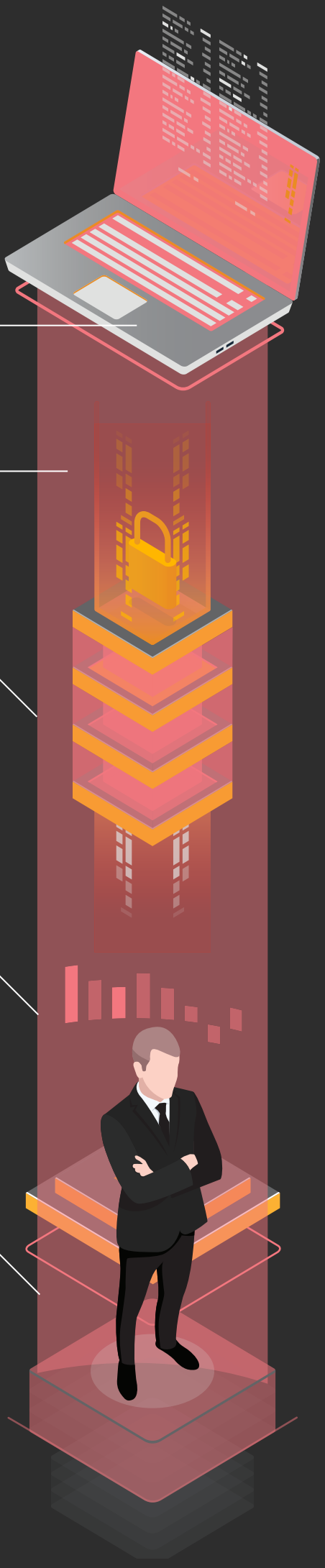
"Personal Data" is defined as any data that may lead to identifying an individual, directly or indirectly. Please see page 10 for further details.

"Data Subject" is defined as an individual to whom the personal data relates.

"Data processing" or **"Processing"** means any automated or manual operation(s) carried out on personal data. In essence, this covers almost any relevant action that could possibly be performed on personal data including, for instance, collecting, recording, saving, indexing, organising, formatting, storing, modifying, updating, consolidating, retrieving, using, disclosing, transmitting, publishing, sharing, linking, blocking, erasing and destroying personal data.

"Competent Authority" is the Saudi regulatory authority that is responsible for enforcing the PDPL. The Saudi Data and Artificial Intelligence Authority (SDAIA) is the Competent Authority as of now. It is expected that the role of the Competent Authority will be undertaken by the National Data Management Office, one of the regulatory bodies of SDAIA.

"Sensitive Data" is a subset of personal data. It is defined as any personal data relating to an individual's racial or ethnic origin, religious, intellectual or political beliefs, criminal and security data, biometric data, genetic data, health data and data that indicates that an individual's parent is unknown. Please see page 11 for further details.



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. Although the PDPL does not explicitly list the principles, such principles are embedded in the PDPL's provisions. Understanding of these principles will help you to understand many of the requirements of the PDPL.

There are seven key data privacy principles that form the fundamental conditions that organisations must follow when processing personal data. Processing personal data in line with these key principles is essential for effective data privacy compliance.

The principles are as follows:

Lawfulness, fairness and transparency

You must always process personal data in a fair, lawful and transparent manner.

Purpose limitation

You must only process personal data for a specific and lawful purpose.

Data minimisation

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

Accuracy

You must ensure that 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 with data privacy laws, regulations and principles.

What is personal data?

Pursuant to the PDPL personal data shall include 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.

Examples of personal data:

- name and surname;
- ID card number;
- online identifiers (e.g. usernames, IP addresses);
- CCTV footage.

Examples of non-personal data

- an organisation's corporate registration number or address;
- mailboxes such as info@pwc.com.

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 are 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, job position.

What is sensitive personal data?

Some personal data is considered sensitive, as it could cause significant harm to an individual if such data is lost, leaked or misused.

Pursuant to the PDPL personal data is classified as “sensitive” if it relates to:

- Health data
- Biometric data
- Genetic data
- Ethnic or racial origin
- Religious, intellectual or political beliefs
- Criminal and security data
- Any data that indicates that an individual’s parent is unknown

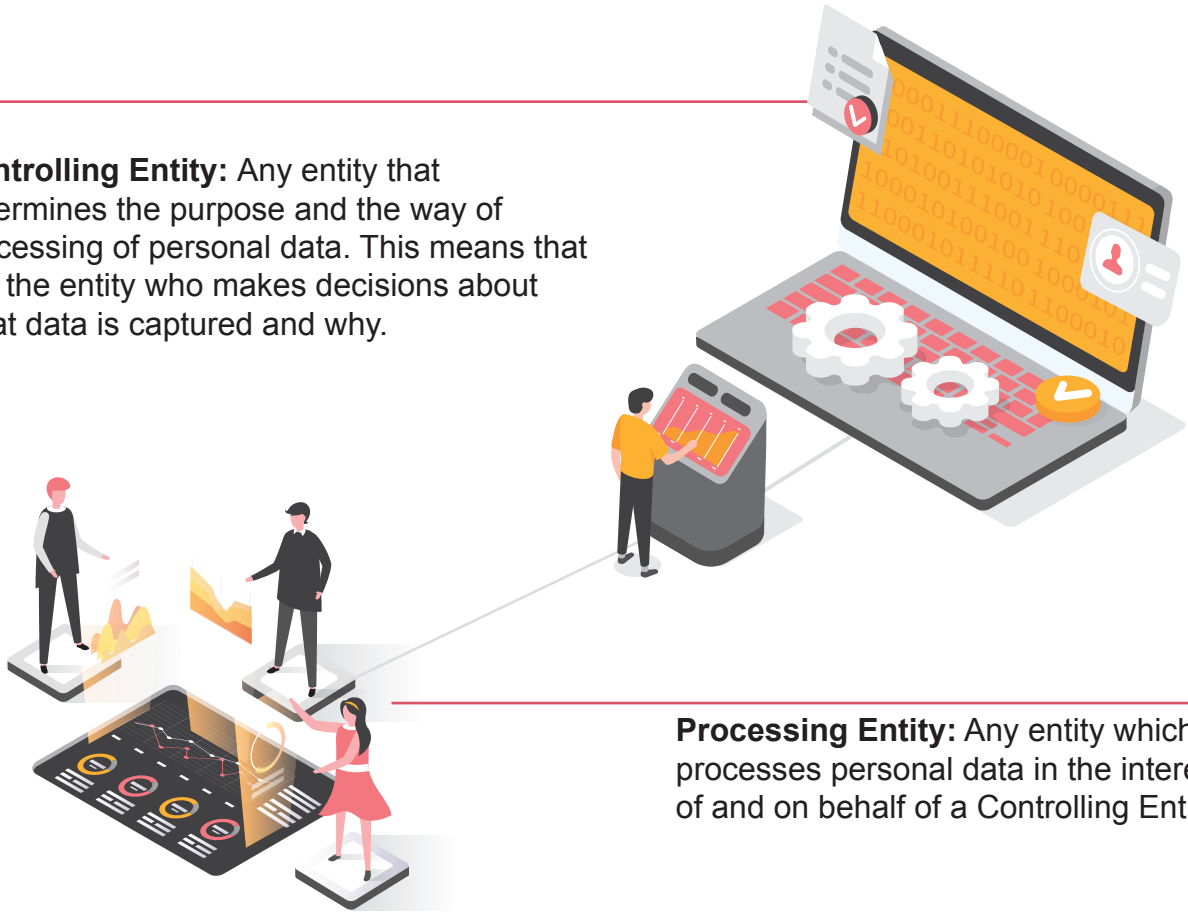
It is important to differentiate between sensitive data and non-sensitive personal data. This is because the use of sensitive data is associated with more restrictions under the PDPL. For instance:

- Legitimate interest may not be used as the lawful basis to process sensitive data.
- The use of sensitive data for marketing purposes is not allowed.
- The unauthorised disclosure of sensitive data could be punished by imprisonment up to 2 years and/or a fine not exceeding SAR 3 million (around USD 800,000).

Controlling Entity vs. Processing Entity

The PDPL draws a clear distinction between “Controlling Entity” and “Processing Entity” to recognise that not all organisations involved in the processing of personal data have the same legal status and responsibilities.

Controlling Entity: Any entity that determines the purpose and the way of processing of personal data. This means that it is the entity who makes decisions about what data is captured and why.



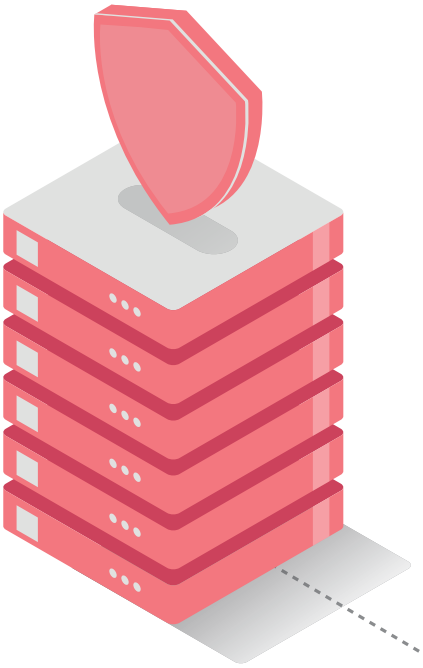
Processing Entity: Any entity which processes personal data in the interest of and on behalf of a Controlling Entity.

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 to order products. The retailer uses a cloud provider to host the website and maintain the customer database. In this case, the retailer is the Controlling Entity and the cloud provider is the Processing Entity.

Am I a Controlling Entity or a Processing Entity?

It is important to note that depending on circumstances an organisation could be a Controlling Entity or a Processing Entity. For instance, it may be acting as a Controlling Entity for some personal data and processing activities, and as a Processing Entity for others.

What does it mean if I am a..



Controlling Entity

You are ultimately accountable for your own compliance and the compliance of your Processing Entities. Your are responsible for full compliance with the PDPL, including with restrictions on the use of personal data and sensitive data, responding to individuals' rights, enforcing security measures, managing data breaches and engaging only Processing Entities who provide sufficient guarantees to protect the personal data.

Processing Entity

You have less autonomy over the personal data that you are processing, but you still have legal obligations regarding processing of such personal data. For example, if you engage a sub-processor, you may be responsible to the Controlling Entity for the sub-processor's compliance with the processing requirements.

Your responsibilities also include compliance with your Controlling Entity's instructions, terms and conditions of the data processing agreement, enforcing security measures, notifying Controlling Entity of personal data breaches, etc.

Data Subject's Rights

One of the aims of the PDPL is to empower individuals and give them control over their personal data. Therefore, the PDPL sets forth a list of the Data Subject's rights. It is important to note that not all of these rights are absolute and some of them only apply subject to meeting specific conditions.

The individuals have the following rights under the PDPL:

Right to be informed

Individuals have the right to be informed about the lawful basis for collection of their personal data, as well as of the purpose (aim) of such a collection.

Right to request correction

Individuals can request to have their personal data corrected (if inaccurate), completed (if incomplete) or updated (if out of date).

Right to request erasure*

Individuals can request erasure of their personal data.

Right to access the personal data

Individuals have the right to access their personal data subject to meeting requirements of the Implementing Regulations and PDPL.

Right to withdraw consent

Individuals can at any time withdraw their consent which they previously gave in relation to processing of their personal data.

Right to request provision of personal data

Individuals have the right to request their personal data to be provided to them in a readable and clear form.

* As mentioned above, not all the rights are absolute. For example, the right to request erasure is often misunderstood, as many assume that their personal data could be erased upon their request without any conditions. However, before the personal data is erased upon the individual's request, certain requirements must be met (depending on particular circumstances). For example, your bank may be required to keep your records for a specific time period under banking laws and regulations, and your request to erase the personal data may not be satisfied by the bank in this case.

When can personal data be processed?

The PDPL allows processing of personal data only if there is a suitable lawful basis in place. The PDPL specifies the **consent of the individual** as the main lawful basis for processing of personal data.

That said, according to PDPL you may process Personal Data **without consent** of the individual in following cases:

- There is a confirmed interest for the individual to perform processing of his/her personal data, and it is difficult or impossible to contact him/her.
- The data processing is required to comply with another law.
- The data processing is required to perform an agreement to which the individual is a party.
- If the Controlling Entity is a public entity and the processing is required for security purposes or to meet judicial requirements.
- If data processing is required to achieve legitimate interests of the Controlling Entity and the processed personal data is not sensitive.

As different types of data require different levels of protection, the PDPL specifies a number of additional conditions for processing health and credit data:

Health data:

- Access to health data should be restricted to the fewest possible number of employees.
- Processing of health data should be restricted to the fewest possible number of employees.

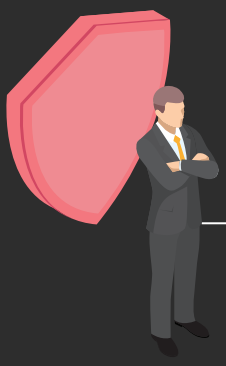
Credit data:

- Explicit consent must be obtained from the Data Subject to process this type of personal data.
- When the Controlling Entity receives a request to disclose credit data, the Data Subject shall be notified.

Top tips

- You should clearly define the lifecycle of the personal data that you use (from collection to deletion) and check all stages of processing of personal data against the requirements of the PDPL.
- You must ensure that for every kind of processing of personal data you have a suitable legal basis (consent or another legal basis).

Ten steps to an effective data privacy programme



1

Appoint a Data Privacy Officer 17

2

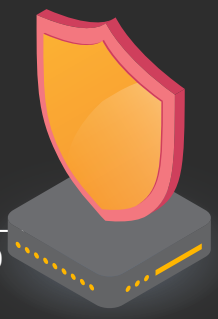
Maintain a personal data register 18

3

Notify purpose and seek consent (where it is required) 19

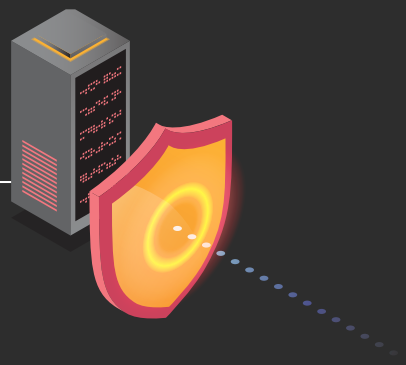
4

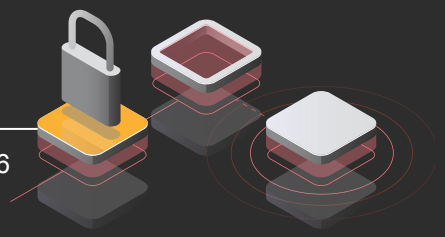
Enforce security mechanisms 20



5

Respond when individuals ask about their personal data 22





1 Appoint a Data Privacy Officer

Many data privacy laws introduce the concept of a Data Privacy Officer (**"DPO"**), a new leadership role for overseeing the organisation's data privacy processes and ensuring compliance with the applicable data privacy laws. Pursuant to the PDPL the Controlling Entity may be required to appoint a DPO in cases determined by the Implementing Regulations.

What's the role of the DPO?

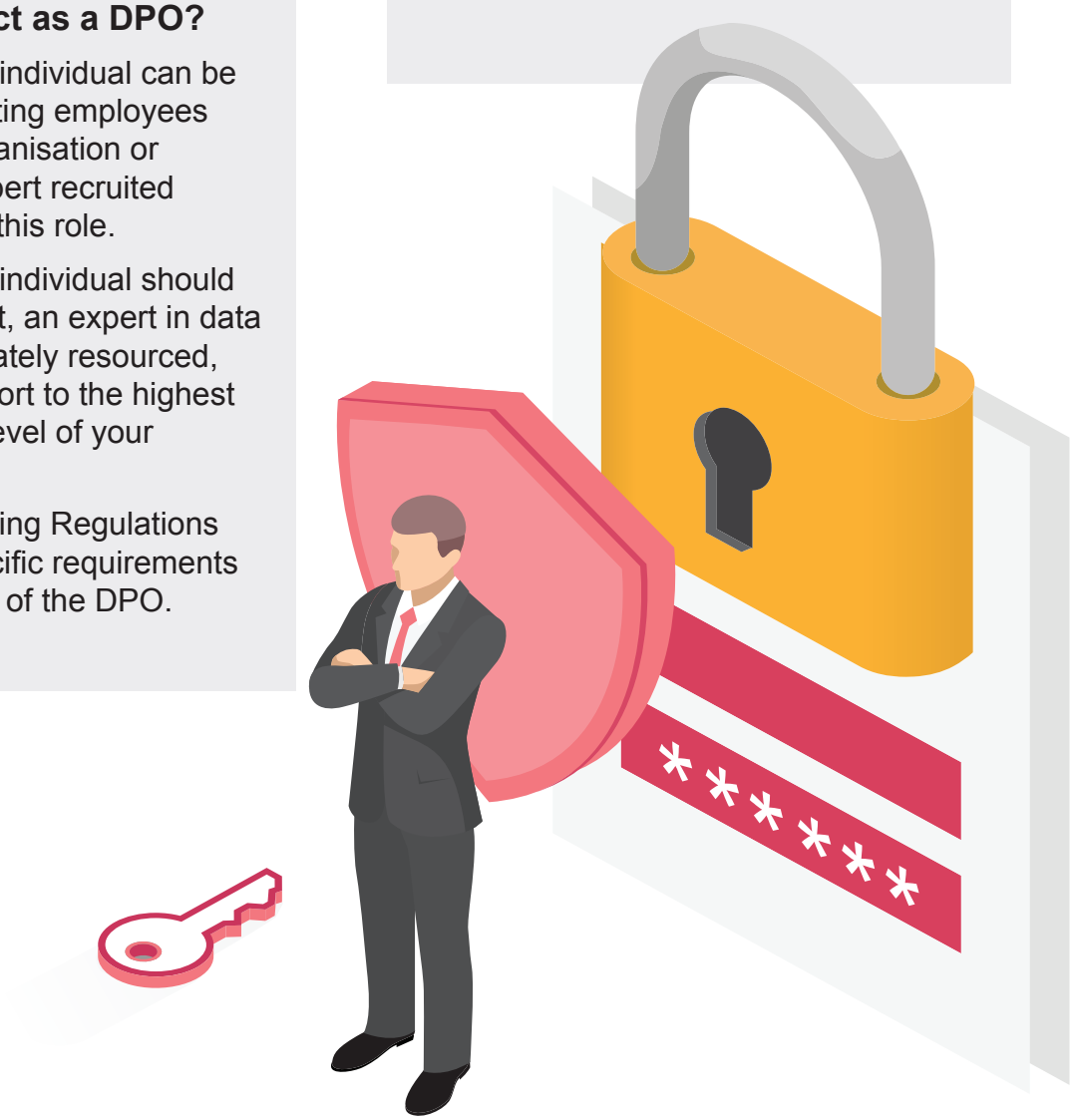
The DPO is the main person who assists your organisation in compliance with data privacy laws and regulations. The DPO is the key point of contact for all data privacy issues within your organisation.

Who could act as a DPO?

The appointed individual can be one of the existing employees within your organisation or an external expert recruited specifically for this role.

The appointed individual should be independent, an expert in data privacy, adequately resourced, and should report to the highest management level of your organisation.

The Implementing Regulations determine specific requirements to appointment of the DPO.



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 activities in your organisation involving personal data and documenting how and why the personal data is used. Such information must be specified in the document called a “Record of Processing Activities”.

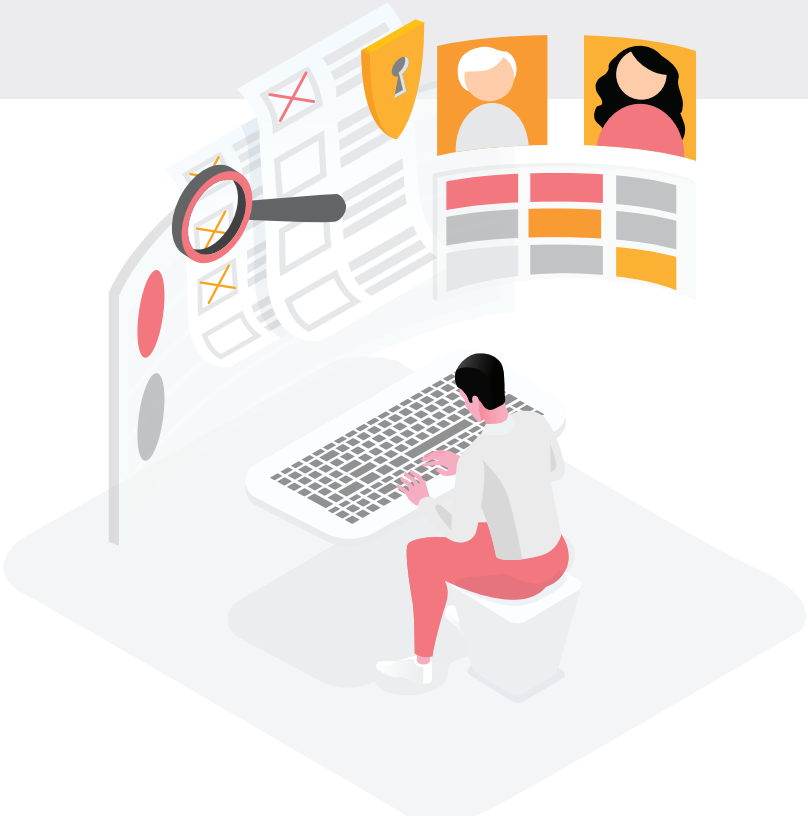
How can I identify personal data being processed?

Maintaining a Record of Processing Activities is one of the key requirements of most data privacy regulations worldwide and it is also required by the PDPL. 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 is located, who has access to it and how long it is retained.

What details should I include in the register?

The PDPL requires you to specify in the register the following information regarding each personal data processing activity within your organisation:

- contact details of the Controlling Entity;
- purpose (aim) of processing personal data;
- description of categories of Data Subjects;
- any organisation to which personal data has been (or will be) disclosed;
- whether personal data has been, or will be, transferred outside Saudi Arabia or disclosed to an organisation outside Saudi Arabia;
- the retention period of the personal data kept by your organisation.



3 Notify purpose and seek consent (where it is required)

The PDPL requires organisations to be transparent about the way that they use personal data. When collecting personal data you must provide their Data Subjects with clear information explaining why, what and how you are intending to process their personal data.

What information do I need to provide to Data Subjects?

The following information must be provided to individuals:

- lawful basis for collecting personal data;
- purpose (aim) of collecting personal data, and whether collecting all or some of the personal data is mandatory or optional, as well as confirmation that the personal data will not be processed later in a manner inconsistent with the purpose of its collection or against requirements of the PDPL;
- identity of the Controlling Entity collecting the personal data and its address, unless the collection is for security purposes;
- entity(ies) to which the personal data will be disclosed, their description and whether the personal data will be transferred, disclosed or processed outside Saudi Arabia;
- possible effects and risks of not completing the personal data collection procedure;
- rights of the Data Subjects, as determined by the PDPL;
- other information, as could be required by the Implementing Regulations.

How to provide the data privacy information?

As a general rule, such information must be provided to individuals at the start of collection of their personal data. The information must be concise, transparent, intelligible, easily accessible and use clear and plain language. To meet these requirements you could consider using a combination of techniques, such as an expandable section approach, dashboards, just-in-time notices, etc.

What is consent?

The generally accepted definition of consent is 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 individuals control and choice over how their personal data is processed. It constitutes one of the ways that entities can lawfully rely upon to process personal data, however, there are conditions that need to be met to ensure that the consent is valid. Such conditions are set out in more detail in the Implementing Regulations.

Please note that **consent is not the only lawful basis** for processing of personal data under the PDPL. Please see details on other lawful bases on page 15.

How can I obtain consent?

- You must ensure that you properly record the consent which an individual provided to you regarding processing his/her personal data. The consent must be distinct from any other agreement (e.g. terms and conditions) and written using clear and simple language.
- Individuals can withdraw their consent at anytime. The consent withdrawal procedure should be as easy as the procedure for giving the consent.

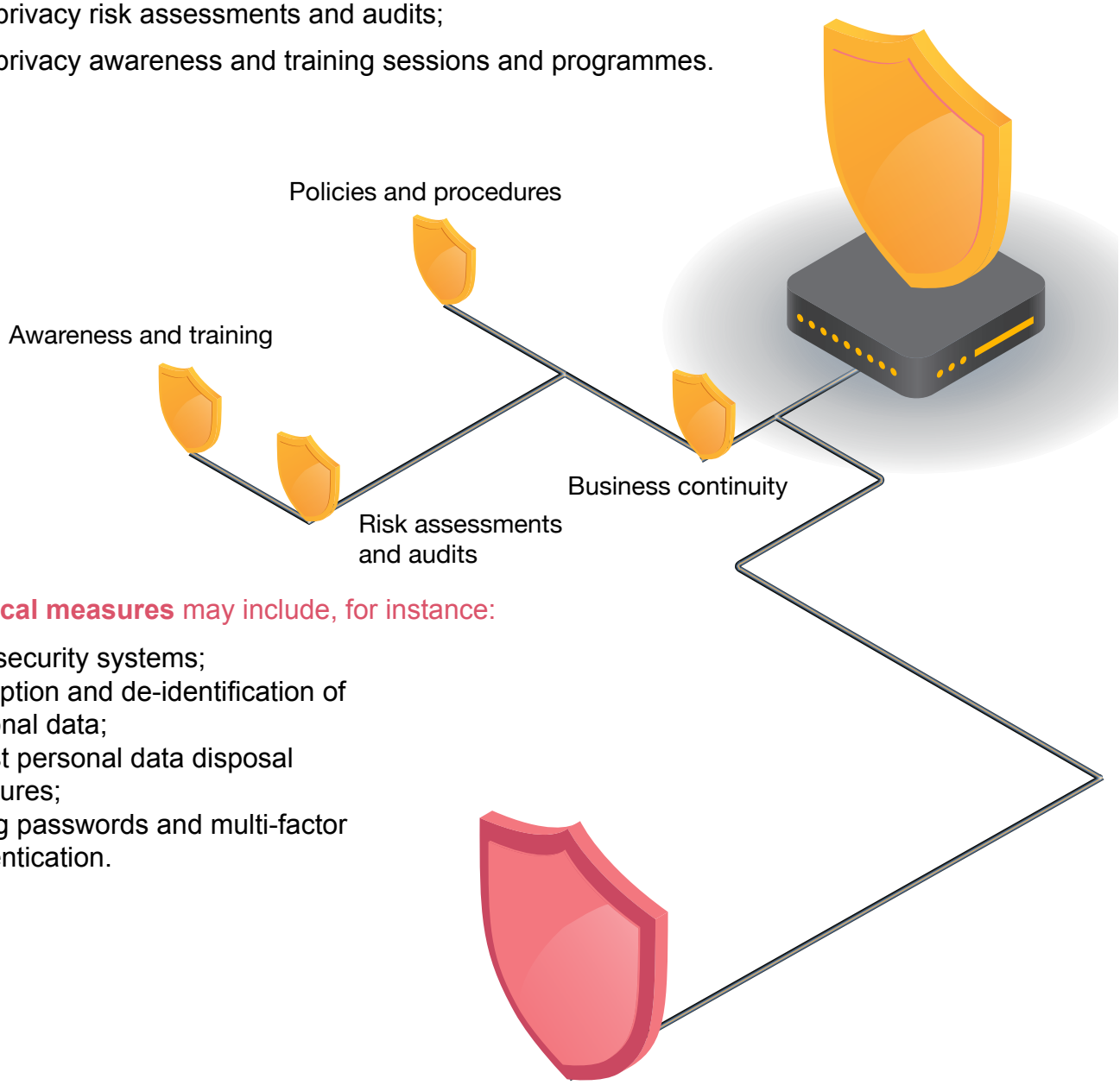
4 Enforce security mechanisms

The PDPL requires the Controlling Entity to take the organisational and technical measures that are necessary to ensure protection of personal data. What is "necessary" must be determined by the organisation itself, taking into account various factors, such as the organisation's size, the amount and types of personal data being processed, etc.

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

Organisational measures may include, for instance:

- internal data privacy policies and procedures;
- business continuity programmes;
- data privacy risk assessments and audits;
- data privacy awareness and training sessions and programmes.



Technical measures may include, for instance:

- data security systems;
- encryption and de-identification of personal data;
- robust personal data disposal measures;
- strong passwords and multi-factor authentication.

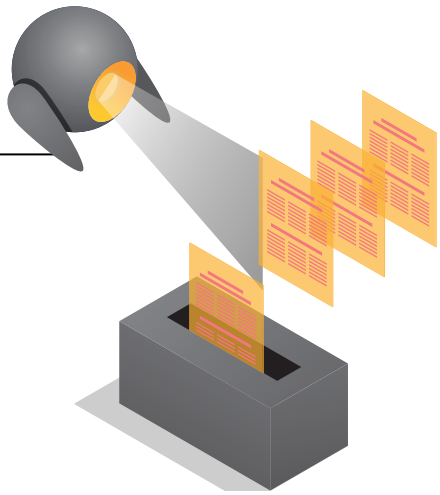
Which security measures should I implement?

Depending on the size of your organisation and the processing activities undertaken, there is a broad range of technical and organisational measures that can support you in protecting personal data. For instance, you may consider utilising established frameworks such as ISO 27001 / ISO 27701 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 basic steps below to determine which measures you should implement:

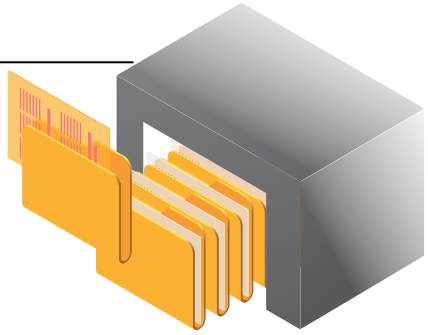
Step 1

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 assessment (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.

5 Respond when individuals ask about their personal data

What are the Data Subjects' requests?

The PDPL introduces new rights for individuals that are designed to give them more control over how their personal data is used. Individuals are entitled to raise requests to exercise their rights and organisations must respond to them within the specific timelines. Such timelines are determined in the Implementing Regulations.

How can I be prepared?

In order to effectively respond to requests of Data Subjects 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 PDPL does not expressly say what information must be specified in the response to the request of the Data Subject. 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 in relation to the requestor;
- the purpose and lawful basis for processing the personal data;
- 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 a Data Subject's request?

1. Identify the request and forward it to the relevant department of your organisation.
2. Verify the identity of the Data Subject who made the request.
3. Assess the request and confirm whether it is based on the PDPL (or another law) and if any specific requirements apply to it.
4. Determine where the personal data of the Data Subject is stored (in specific systems, in hard copies of documents, etc.).
5. Perform the appropriate action according to the nature of the request (e.g. arrange a copy of personal data, erasure of the personal data, etc.).
6. Send and document the appropriate response to the Data Subject.

6 Embed data privacy into your systems, processes and services

The PDPL requires the Controlling Entity to conduct assessments of data privacy risks in relation to every product or a service offered to the general public. This is similar to the concepts of "Data Protection Impact Assessments" and "Privacy by Design" which we see in many other data protection laws. 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 fully and correctly reflect the processing activities).

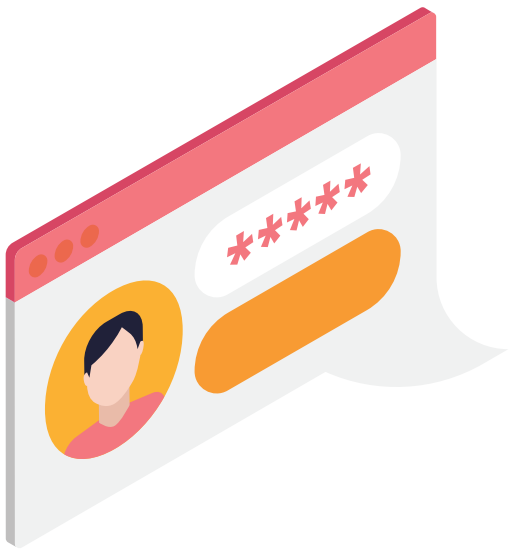
3. Safeguards are established and enabled (example: applying encryption and data minimisation mechanisms on personal data).

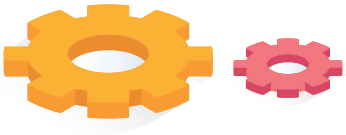
While these principles help to inform the organisation's overall approach, successful privacy by design and default is facilitated by governance and oversight, implemented by supportive work-force.

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, for instance:

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

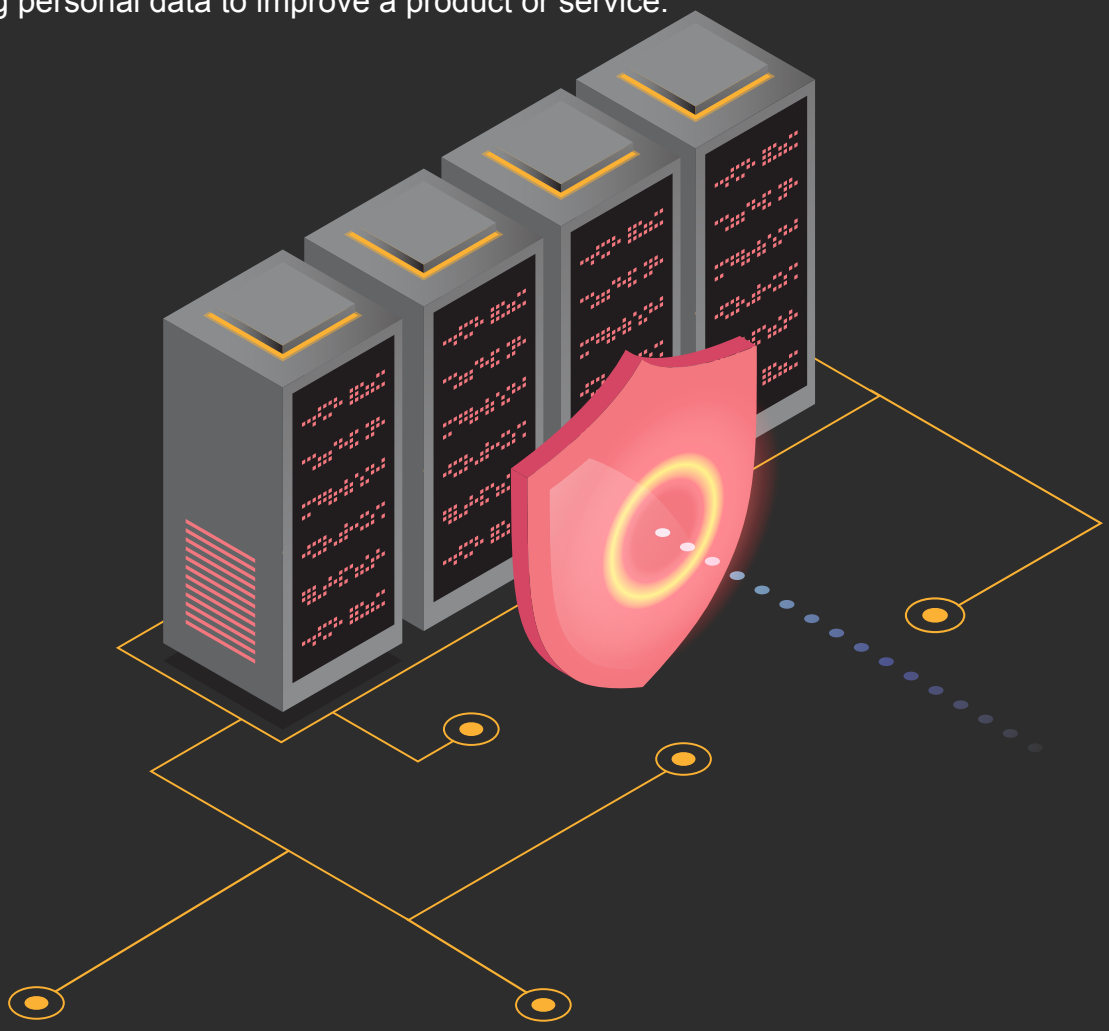




What is “data privacy by design”?

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

- using a new way of storing data (e.g. cloud solutions);
- engaging outsourcers to manage and maintain an IT system;
- new or changing business process;
- new product offering;
- new use of existing personal 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;
- embed controls into your processing activities so that you protect individuals’ data privacy rights.

Privacy by design is mainly comprised of two distinct elements:

1. Data Privacy Impact Assessment (DPIA): an instrument 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

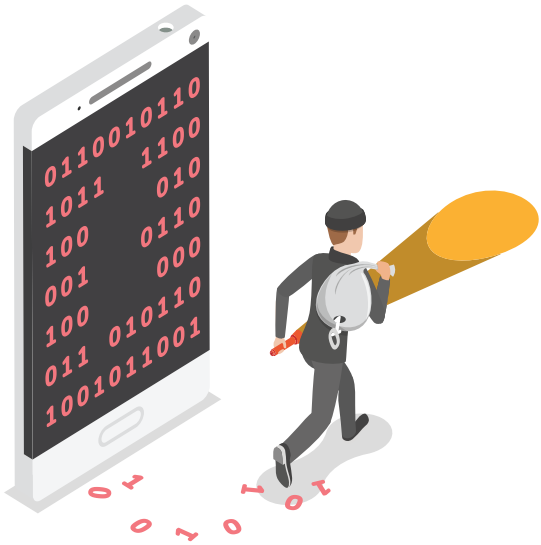
Data breaches can happen for various reasons, despite all the precautions that you may take. The PDPL requires Controlling Entities to notify the Competent Authority and Data Subjects if the data breach takes place – e.g. the personal data is lossed or disclosed in an unauthorised way. Specific procedures on notifying the data breach are determined in the Implementing 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 data breach has been discovered, you must:

- 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 Data Subjects

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:
  - What happened to the personal data in question?
  - What caused the breach?
  - Who are the affected Data Subjects?
  - Description of the estimated impact and possible effects.
- Contact details of your DPO.
- 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.
- Have a response plan in place and communicate it in advance to all employees and third parties (where applicable).
- Allocate the responsibility for managing breaches to a dedicated person or team.
- Regularly test the plan to minimise the disruption that typically follows a breach.

8 Manage third parties

The PDPL requires Controlling Entities to ensure that the third parties who process personal data for them (Processing Entities) have in place proper measures to ensure processing of personal data in accordance with the PDPL. If you engage a third party to process personal data, you may be held liable if it violates the PDPL while providing the services to you.

What should I include in a contract with the Processing Entity?

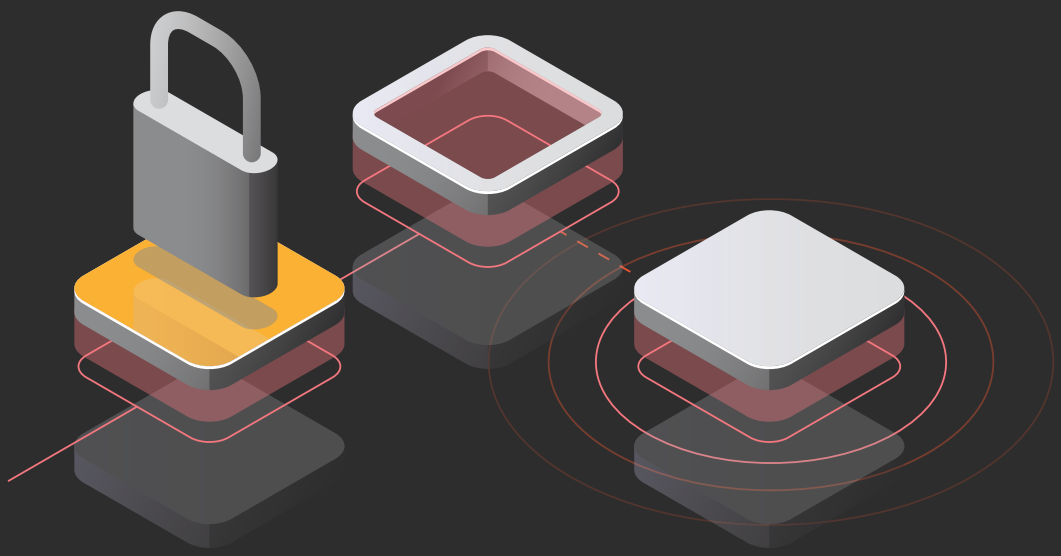
Contract with the Processing Entities shall at a minimum include the following:

- subject-matter and duration of processing;
- nature and purpose of processing;
- types of personal data and categories of Data Subjects subject to processing;
- obligations and rights of the parties – including in the area of cooperation while fulfilling the requirements of the PDPL;
- timelines of the processing;
- liability of the parties;
- Controlling Entity's rights to conduct an audit in relation to the Processing Entity (to assess its compliance with the contract and with the PDPL).

Enhancing your risk management programme related to third parties

Contracts alone are not enough to manage risks associated with engaging third parties. For instance, you may take the following additional steps to enhance your risk management programme:

- Conduct an onboarding assessment to ensure that the third party has adequate controls in place to protect personal data and to comply with the PDPL.
- Continue to improve ongoing monitoring through risk assessments and audits to ensure that third parties are maintaining adequate controls to protect personal data.



9 Comply with cross-border data transfer rules

The updates to the PDPL that were adopted in March 2023 changed the approach to cross-border transfers of personal data. As of now the **PDPL permits the transfer of personal data outside Saudi Arabia, including** its disclosure to the entities located in other countries, than Saudi Arabia. That said, the PDPL requires that certain conditions must be met prior to transferring personal data abroad.

Firstly, the transfer must serve one of the following purposes:

1. The transfer is required for performance of an obligation under an international agreement to which Saudi Arabia is a party.
2. The transfer serves the interests of Saudi Arabia.
3. The transfer is required for performance of an obligation to which the Data Subject is a party.
4. The transfer is required for other purposes (aims), as determined in the Implementing Regulations.

Secondly, the transfer must meet the following conditions:

1. The transfer does not relate to national security or vital interests of Saudi Arabia.
2. The country to which the personal data is transferred has a proper level of protection of personal data – not less than the level as determined by the PDPL and the Implementing Regulations (as such level will be assessed by the Competent Authority*).
3. The personal data will be transferred in the minimal possible amount.

The transfer may be possible without meeting the above conditions if it is necessary for saving the individual's life or his/her vital interests or prevention, studying or treating infection diseases. The Implementing Regulations provide for more details on regulation of cross-border transfers. They also determine the cases when the Controlling Entity could be exempted from meeting the cross-border transfer conditions (including from the condition on transferring personal data only to the country having proper level of protection of personal data).

* It is expected that the Saudi authorities shall determine the "white list" of countries which will be considered as having an adequate level of protection of personal data.

10 Communicate your data protection policies, practices and processes

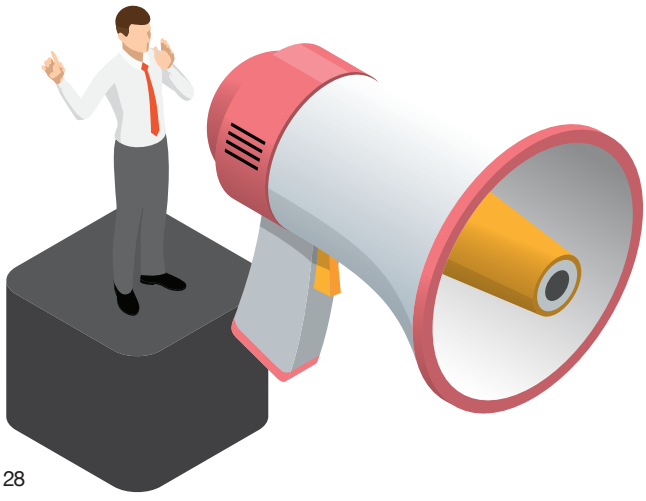
Complying with data privacy laws is not something that can be left to selected departments of your organisation alone. Compliance with data privacy laws requires that everybody in the organisation understands their data privacy responsibilities. It is very important to communicate your data privacy policies 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 DPO easily accessible so that your customers know who to contact for inquiries or complaints.
- Provide information about your data protection policies, practices and complaints processes at the web-site of your organisation.
- 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; and
  - 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 them to repeated practices.
- Use posters, email and other communication tools to raise awareness of the importance of data privacy among all of your employees.
- Ensure that the key employees who handle personal data attend regular data privacy trainings, so that they are kept up to date with your internal processes and latest developments in the data 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

Personal data discovery

What you will get

- Data privacy enhancement project plan
- Record of Processing Activities

Design the future state

Gap assessment

What you will get

- Gap assessment report on the current data privacy capabilities of your organisation
- Road map with recommendations on how to mitigate the identified risks

Target operating model

What you will get

- Report with description of the target data privacy function within your organisation
- Description of how various data privacy stakeholders within your organisation should cooperate with each other

Programme implementation

Possible areas of focus

- 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

- Ongoing consulting on various data privacy issues
- Support in identifying further opportunities on how to enhance data privacy capabilities of your organisation

Get in touch

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

Matthew White
Partner, Cybersecurity and Digital Trust Leader
+971 56 113 4205
matthew.white@pwc.com
linkedin.com/in/mjwme
@mjw0610

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

Oliver Sykes
Partner, Technology Consulting
+971 56 480 2447
oliver.sykes@pwc.com
linkedin.com/in/osykes/

Khaled Kabbara
Partner, Cybersecurity and Digital Trust
+966 54 872 7472
khaled.kabbara@pwc.com
linkedin.com/in/khaledkabbara

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

https://www.pwc.com/m1/en.html

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 152 countries with over 320,000 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(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.