

# Data privacy handbook for the United Arab Emirates

A guide to compliance with the  
UAE's Data Protection Law



**pwc**





# Contents

**04**

A quick introduction to data privacy



**06**

About this handbook



**07**

Why is data privacy important?



**08**

Key concepts



**09**

Key principles of data privacy



**10**

What is personal data?



**11**

What is sensitive personal data?



**12**

Data Controller vs. Data Processor



**14**

Data Subject Rights



**15**

When can personal data be processed?



**16**

Ten steps to an effective data privacy programme



# 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 information with third parties without the individual’s consent. It doesn’t mean that marketing is now forbidden under the UAE 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 cyber attacks and data breaches but fail to understand what else is required under the UAE Data Protection Law.





In the past year there were a 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 November 2021, the United Arab Emirates issued the Federal Law No. 45 of 2021 (the UAE Data Protection Law), which set stricter standards for data privacy and protection and further increased awareness around the importance of data protection compliance.



# 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 UAE Data Protection Law means that there will be a significant impact to organisations which operate or do business with the United Arab Emirates because they will need to develop data privacy programmes to meet the requirements of the law.

We've put together this data privacy handbook to try to simplify the requirements and help you kick-start your data privacy compliance journey.

This handbook reflects the requirements of the UAE Data Protection Law and PwC's own proprietary frameworks. 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 UAE Data Protection Law references "Executive Regulations" which will be issued within six months from the date of issuance of the law (i.e. around May 2022). These "Executive Regulations" will give extra detail about how organisations should comply with the law. We will identify where the regulations impact our guidelines and update this handbook accordingly.

# Why is data privacy important?

Companies that fail to protect personal data and comply with the UAE Data Protection Law aren't just risking penalties enforced by the Office (the regulator). They also risk operational inefficiencies, intervention by regulators and most importantly permanent loss of consumer trust. While the UAE Data Protection Law gives the Office powers to impose penalties, it will not be clear on exactly what the extent of these penalties will be until the Executive Regulations are issued.

## Regulatory

Data protection regulators may enforce mandatory audits, request access to documentation and evidence or even mandate 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

Data Protection Laws across the globe impose heavy financial penalties on businesses that breach the law. In the Middle East it is also common for Data Protection Laws to impose criminal sanctions. We will need to wait to see exactly what penalties are included in the Executive Regulations.

## Operational

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

**'Data processing'** or **'Processing'** means any operation or set of operations performed on personal data through electronic means, including other processing methods. This process includes collecting, storing, recording, organising, adapting, modifying, circulating, transferring, retrieving, exchanging, sharing, using, describing, and disclosing personal data by broadcasting, transfer, distributing, making available, coordinating, merging, restricting, obfuscating, deleting, destroying, or modeling the data.

**'The Office'** is the "Emirates Data Office" established as a result of Federal Decree No. 44 of 2021. The Office is the defacto regulator for the UAE Data Protection Law.

**'Data Subject'** is the natural person who is the subject of the Personal Data. For ease, you can think of this as an individual to which personal data belongs.

**'Personal data'** is defined as information that relates to an identifiable person, either directly or indirectly. Refer to page 10 for further details.

**'Sensitive personal data'** is a subset of personal data and is defined as any data that directly or indirectly reveals a natural person's family, ethnicity, political or philosophical views, religious beliefs, criminal record, Biometric Data, or any data related to that person's physical, psychological, mental, genetic or sexual health. This includes information related to healthcare service provisioning that can reveal the person's health status. Refer to 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 UAE Data Protection Law does not explicitly list the principles within the law, the principles are embedded in the requirements and an understanding of these principles will help you understand many of the law's requirements.

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 good data protection.

## The principles are:

### Lawfulness, fairness and transparency

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

### 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.

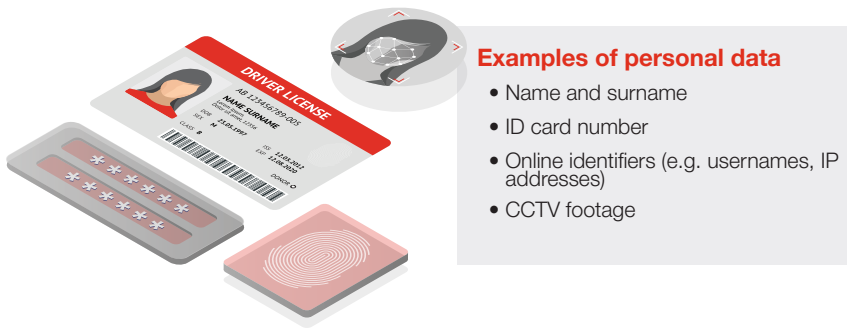
### Accountability

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 either a living person, either directly or indirectly. 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. Example: name, ID number, email address.
- Indirectly, if different sets of data from different sources, when combined, could identify a specific person. Example: gender, birth date, licence plate number.

# What is sensitive personal data?

Some personal data is considered sensitive, as it could cause harm to the individual if leaked or misused.

Under the UAE Data Protection Law, personal data is classified as 'sensitive' if it directly or indirectly reveals a person's:

- » Family
- » Ethnicity
- » Political or philosophical views
- » Religious beliefs
- » Criminal record
- » Biometric Data
- » Data related to that person's physical, psychological, mental, genetic or sexual health including any information that can reveal the person's health status.

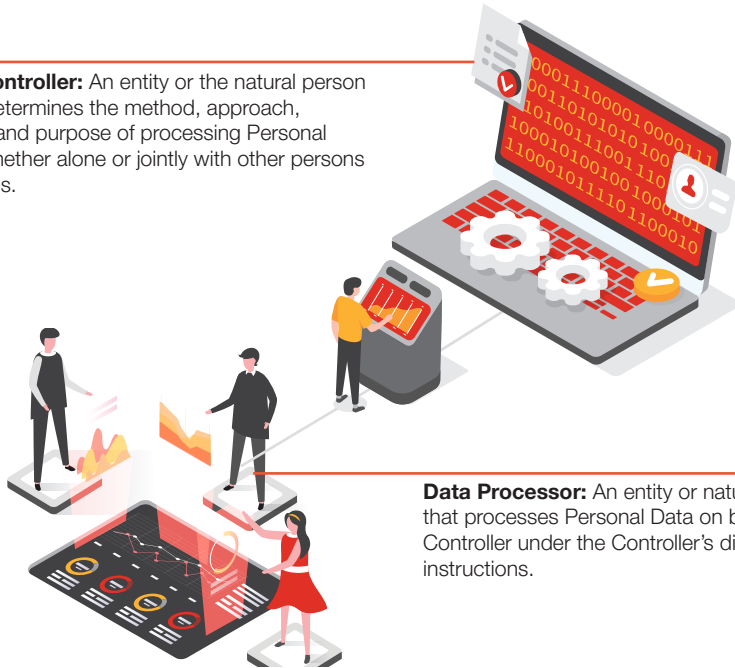


It's important to differentiate between personal data and sensitive personal data because the processing of sensitive personal data usually requires additional safeguards to be in place. The details about these safeguards are likely to be covered in the Executive Regulations.

# Data Controller vs. Data Processor

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

**Data Controller:** An entity or the natural person which determines the method, approach, criteria, and purpose of processing Personal Data, whether alone or jointly with other persons or entities.



**Data Processor:** An entity or natural person that processes Personal Data on behalf of the Controller under the Controller's direction and instructions.

A simple way to think about this is as follows: A retailer creates an e-commerce website and decides what information they require from customers to create an account. The company uses a cloud provider to host their website and database. In this case, the company is the Data Controller and the cloud provider is the Data Processor.

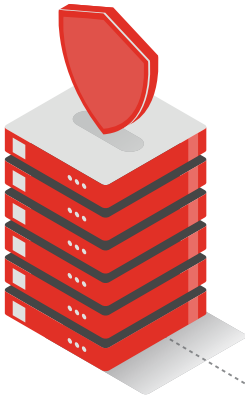
## Am I a Data Controller or a Data Processor?

It is important to note that an organisation is not by its nature either a Controller or a Processor. It may be acting as a Data Controller for some personal data and processing activities, and as a Processor for others.

# What does it mean if I am a..

## Data controller

You are ultimately accountable for your own compliance and the compliance of your processors. Your responsibilities include compliance with the UAE Data Protection Law, the data protection principles, responding to individuals' rights, enforcing security measures, managing data breaches and engaging only with processors providing sufficient guarantees to protect the data.



## Data 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 Data Controller for the sub-processor's compliance.

Your responsibilities include compliance with your Data Controller's instructions as set out in third party contracts, enforcing security measures, notifying the Data Controller of personal data breaches and not engaging any sub-processor before the approval of the controllers.

# Data Subject Rights

One of the aims of data privacy laws is to empower individuals and give them control over their personal data. Therefore, UAE Data Protection Law refers to a number of rights concerning the protection of individuals' personal data. It's important to note that not all of these rights are 'absolute', meaning some only apply in specific circumstances.

## Right to delete

Individuals can request for their personal data to be deleted without undue delay.

## Right to object to automated decision making

Individuals can object to decisions made about them based on automated means. They also have the right to obtain human intervention to review decisions made which were based on automated processing.

## Right to correct

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

## Right of access to information

Individuals have the right to be informed about what data is being processed and how it is being processed.

## Right to request transfer

Individuals have the right to obtain their personal data in a machine-readable format and the individual the right to request that transfer of their data to another controller.

## Right to restrict processing

Individuals have the right to compel the Controller to restrict, suspend or stop the processing of their data.



\* As mentioned above, not all personal data owners rights are 'absolute'. The 'right to request deletion' is often misunderstood. The main reason for this is because many assume that it is an 'absolute right' whereas in actual fact there are only certain circumstances that people can request for their data to be deleted. For example, your bank may be required to keep records of your account for a given time period and your right to destruction does not supercede this (i.e. the bank can refuse to delete this data as they are required to keep it).

# When can personal data be processed?

The UAE Data Protection Law prohibits the processing of Personal Data without obtaining the consent of the Data Subject. However, the Law provides exceptions to this requirement and permits the processing of personal data in the following cases:

**Public interest and public health:** The processing is necessary to protect public interest or public health.

**Publicly available information:** The processing relates to Personal Data which are made public by the Data Subject.

**Defence of legal claims:** The processing is necessary for the defence of legal claims.

**Preventive or occupational medicine:** The processing is necessary for the assessment of an employee's ability to perform work.

**Archiving, scientific or historical research:** The processing is necessary for achieving purposes, scientific, historical or statistical research.

**Legal obligations:** The processing is necessary for the Controller to carry out their legal obligations in the fields of recruitment, social security or social protection or in compliance with other laws in the UAE.

**In the interest of the Data Subject:** The processing is necessary to protect the interests of the Data Subject.

**Contractual obligations:** The processing is necessary for the performance of a contract to which the Data Subject is party.

The Law also allows for other cases to be specified in the Executive Regulations.



# Ten steps to an effective data privacy programme



1

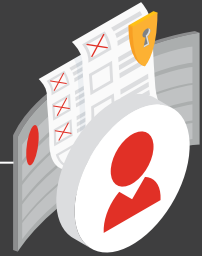
Appoint a Data Protection Officer

18

2

Maintain a personal data register

19



Notify purpose and seek consent

20

3

4

Respond when individuals ask about their personal data

21



5



Enforce security mechanisms

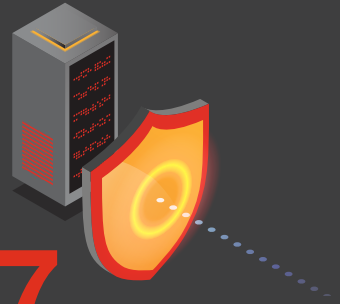
22



# 6

Embed data privacy into your systems, processes and services

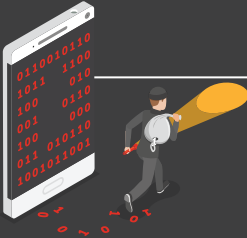
24



# 7

Notify data breaches

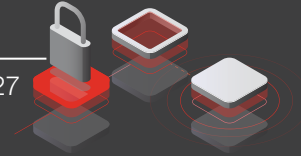
26



# 8

Manage third parties

27



# 9

Protect personal data when transferring across borders

28



# 10

Communicate your data protection policies, practices and processes

30



# 1 Appoint a Data Protection Officer

The UAE Data Protection Law introduces the concept of a 'Data Protection Officer' (DPO), a new leadership role for overseeing the organisation's data protection programme and ensuring compliance with applicable data protection laws. The UAE Data Protection Law requires Data Controllers and Data Processors, in some circumstances, to appoint an individual within the organisation to be responsible for the organisation's commitment to implement the provisions of the Law.

## What's the role of the appointed individual?

The appointed individual will assist you in monitoring internal compliance with the UAE Data Protection Law, 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.

## Who could act as an appointed individual?

The appointed individual can be an existing employee of, or may be authorised by, the Data Controller or Data Processor.

The Data Protection Officer must have sufficient skills and expert knowledge in Data Protection.



# 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 often called a 'Record of Processing Activities' or 'RoPA'. This is a requirement for both Data Controllers and Data Processors.

## 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's also a required under the UAE Data Protection Law. 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?

The UAE Data Protection Law requires you to identify and document the following for every processing activity within your organisation:

- The contact details of both the Data Protection Officer and the Data Controller or Data Processor
- The purpose of the personal data processing activity
- A description of the categories of personal data
- The details of people authorised to access the personal data
- The mechanism for erasing, modifying or processing the personal data
- The details of technical and organisational measures in place to protect the personal data
- Whether personal data has been, or will be, transferred outside the UAE
- The retention period for keeping the personal data



# 3 Notify purpose and seek consent

The UAE Data Protection Law requires the processing of Personal Data to be fair, transparent and lawful. When collecting individuals' personal data you must provide them with clear information explaining why, what and how you're intending to process their personal data.

## What information should I provide?

In order to meet the requirements in the UAE Data Protection Law around transparency we recommend that the following should be included in the privacy notice shared with individuals:

- Details about what personal data is being collected or processed
- The purpose of processing and legal reason for collecting it
- The method of collecting the personal data
- The means of storing the personal data
- How long the data will be processed and when it will be destroyed
- The rights of the Data Subjects and how those rights can be exercised
- The contact details of your organisation and Data Protection Officer
- Recipients of personal data and details of cross-border transfers

## How to provide it?

Privacy information should be provided to individuals at the time of collecting their personal data, or within a reasonable timeframe if collected from other sources. Privacy 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 and just-in-time notices.

## What is consent?

Valid consent under the UAE Data Protection Law is a clear, simple and unambiguous agreement provided by an individual. The consent should also include a reference to the right of the Data Subject to withdraw his consent.

Consent means giving people control and choice over how an individual's personal data is processed. It constitutes one of the ways that entities can lawfully process personal data. Where processing is based on consent, the Data Controller must be able to demonstrate that the Data Subject consented to the processing. In other words, the Data Controller must maintain a register of inventory of the consents captured.

## How can I obtain consent?

- Individuals can give their consent in written or electronic form. The consent should be distinct from any other agreement (e.g. terms and conditions) and written using clear, simple and unambiguous language.
- Individuals can withdraw their consent at anytime, and the withdrawal procedures should be as easy as those for giving the consent.



# 4 Respond when individuals ask about their personal data

## What are Data Subject Requests?

The UAE Data Protection Law introduces new rights for individuals that are designed to give them more control over how their data is used. These are referred to as “Data Subject Requests”. Individuals are entitled to raise requests to exercise their data subject rights, free of charge, and organisations must respond. Many data protection laws specify a period of time within which the organisation must respond and this is something we may see in the Executive Regulations.

## How can I be prepared?

Your organisation should implement robust procedures to authenticate the requester, assess the validity of the request and formulate an adequate response.

## What information should I provide?

- What personal data is being processed. Refer to page 10 for further details.
- The purposes for processing the data.
- Details of how the personal data is processed.
- Any decisions made through automated processing.
- Details of any third party recipients of the Personal Data.
- Details of any cross-border data transfers.
- 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 request?

1. Receive the data subject 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. Determine where the personal data of the individual is stored, be it in systems or physical documents.
4. Perform the appropriate action according to the type of data subject request (i.e. copy data, delete data, restrict processing etc).
5. Provide appropriate details to the DPO for delivery and response to the data subject.
6. Send and document the appropriate response to the individual.

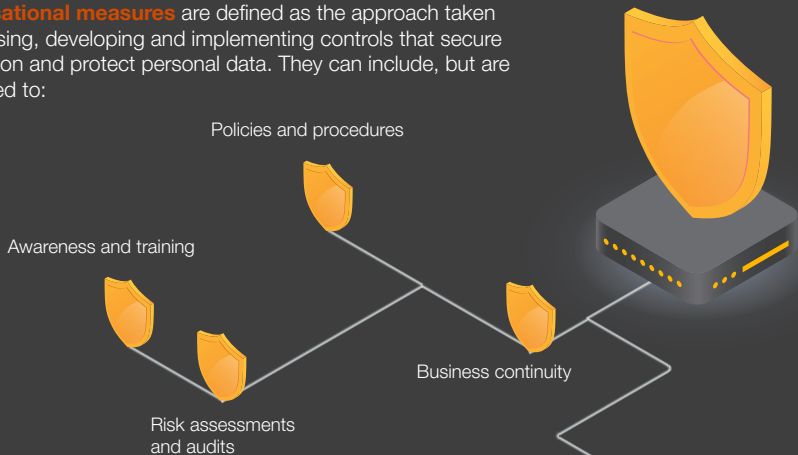


# 5 Enforce security mechanisms

The UAE Data Protection Law requires both the Data Controller and the Data Processor to take the necessary steps to prevent unauthorised disclosure of personal data. This means that organisations need to take reasonable steps to protect personal data. What is “reasonable” will usually come down to a business decision with the support of legal counsel, and will be based 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 information that you process.

**Organisational measures** are 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:



**Technical measures** are defined as the measures and controls implemented on systems from a technological aspect. Protecting such aspects is vital to data security, but goes above securing access to devices and systems. They can include, but are not limited to:

- System and physical security
- Encryption or de-identification of personal data
- Robust data disposal measures
- Passwords and two-factor authentication
- Bring your own device (BYOD) and remote access



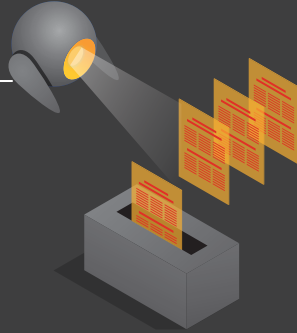
## Which security measures should I implement?

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 / ISO27701 to assess and develop adequate measures.

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

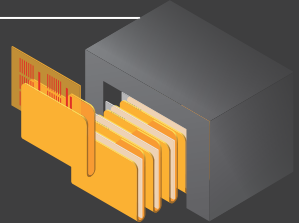
### Step 1

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 UAE Data Protection Law includes requirements for the Data Controller to conduct assessments relating to the impact of personal data processing and to apply appropriate technical and organisational measures by default. These concepts are commonly described as “Data Protection Impact Assessments” and “Data Privacy by Design and by Default”, respectively. 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.
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.

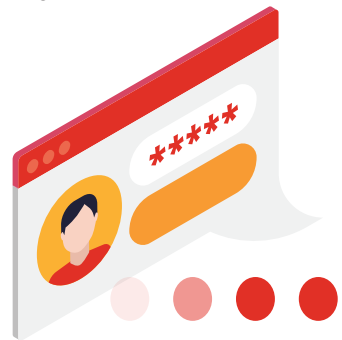
Privacy by default requires you to ensure that you only process personal data that is necessary to achieve your specific purpose, while considering things like:

- 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 third party 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.
- Embed controls into your processing activities so that you protect individuals' rights.



## Privacy by design is mainly comprised of two distinct elements:

- Data Privacy Impact Assessment (DPIA): a tool used to identify and manage data privacy risks.
- 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 UAE Data Protection Law includes breach notification requirements where Data Controllers must immediately notify The Office (the regulator) if they experience a data breach. Further, if the data breach would have an impact on the privacy, confidentiality or security of the Data Subject's data, the Controller must notify the Data Subject.

## 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
- Determine if the breach impacts the privacy, confidentiality or security of the Data Subject's personal data
- Determine if you need to notify The Office (the regulator) and individuals concerned
- Carry out a thorough investigation to identify the source of the breach



## Notifying The Office

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



- Nature of breach
- What caused the breach
- Approximate number of records or data subjects affected
- Details of the Data Protection Officer
- Possible and expected impacts of the breach
- The things you did to investigate and remediate the incident.

## Top tips when dealing with data breaches

- 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 (where applicable) third parties
- 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 UAE Data Protection Law requires Data Controllers to ensure that the third parties or suppliers to whom they transfer Personal Data (i.e. Data Processors) implement appropriate safeguards to satisfy the requirements of the UAE Data Protection Law and ensure ongoing compliance with it. If you engage a third party to process personal data, you may be held responsible if your service provider violates the requirements of the law while providing the service to you.

When entering into a contractual agreement with a third party service provider, ensure there are clauses that require them to take sufficient measures to ensure compliance with the requirements of the UAE Data Protection Law and any other applicable data privacy laws.

### What should I include in a contract?

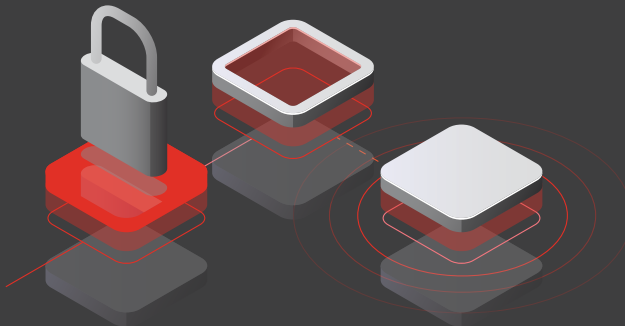
Contractual agreements with third parties should at a minimum include the following details:

- The scope, nature and purpose of processing
- The type of personal data and categories of data subjects
- The minimum terms or clauses required of the processor
- The obligations and rights of the controller
- The obligations of the Data Processor to erase or hand over the data at the end of the contract

### Enhancing your third party risk management programme

Contracts alone are not enough to manage third party risks. Outlined below are additional steps you can consider to enhance your third party risk management programme:

- Conduct a due diligence assessment to ensure that the third party 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 third parties are maintaining adequate controls to protect personal data.
- Ensure that you understand whether any of your third party Data Processors are engaging with any sub-processors and ensure appropriate safeguards are put in place.



# 9 Protect personal data when transferring across borders

The UAE Data Protection Law permits the transfer of personal data outside the UAE under the following conditions:

- The country to which the data is being transferred has local legislation that includes the main provisions, measures, controls, conditions and rules for protecting the confidentiality and privacy of the Personal Data, including the Data Subject's individual rights.
- The country to which the data is being transferred has bilateral or multilateral agreements with the UAE in relation to data protection.

It is common for Data Protection Regulators to issue 'whitelists' which specify which countries they accept have adequate levels of protection in place for Personal Data. This is something that we may see in the Executive Regulations or in guidance issued by The Office.



## Can I transfer Personal Data to a country which does not have an adequate level of protection?

The Law includes exceptions which permit the transfer of Personal Data to countries which do not have an adequate level of protection. These exceptions include:

**Contractual safeguards:** A contract or agreement which applies the provisions, measures, controls and requirements of the UAE Data Protection Law can be signed between the two organisations transferring the data.

**Express consent:** The Data Subject can provide his/her express consent to the transfer outside of the country.

**Contractual obligations:** Where the transfer is necessary for the conclusion or performance of a contract between the Data Subject and the Controller, or the Data Controller and a third party, where it is in the interests of the Data Subject.

**Legal and judicial obligations:** Where the transfer is necessary to carry out obligations and to prove, exercise or defend rights before the judicial authorities. It is also permitted if the transfer is necessary for the implementation of a procedure relating to an international judicial cooperation.

**Public interest:** The transfer is necessary for the protection of the public interest.



# 10 Communicate your data protection policies, practices and processes

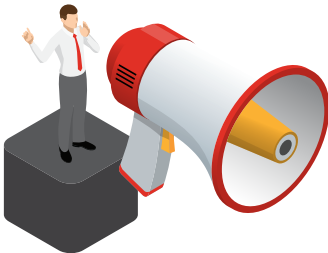
Complying with the UAE Data Protection Law is not something that can be left to the legal and compliance departments alone. Compliance with data privacy laws requires that everybody in the organisation understands their responsibilities to protect personal data. It is very important to communicate your 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 DPO 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 space.



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

# 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, Cybersecurity and Digital Trust  
+971 56 480 2447  
oliver.sykes@pwc.com  
www.https://www.linkedin.com/in/osykes/



**Richard Chudzynski**

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





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](http://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](http://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](http://www.pwc.com/structure) for further details.

© 2021 PwC. All rights reserved