pwc

# Data privacy & responsible AI handbook for the UAE

## A guide based on UAE laws and regulations

# Table of contents

# About this handbook

We have put together this data privacy handbook to simplify the requirements of the United Arab Emirates (UAE) Personal Data Protection Law (PDPL) and help organisations kick-start and strengthen their data privacy compliance journey.

This handbook is designed around the UAE federal data protection framework, providing a practical and accessible guide to its key requirements. Separate handbooks may be published in due course to cover the specific requirements of the Dubai International Financial Centre (DIFC) Data Protection Law and the Abu Dhabi Global Market (ADGM) Data Protection Regulations. However, many core elements of a robust data protection and AI governance program, such as governance structure, risk assessments, data subject rights, security measures, accountability and transparency, are similar across these regimes. Accordingly, while this handbook is centred on the federal regime, the principles and practical steps outlined here will also be relevant when designing or enhancing data protection and AI programs in organisations subject to DIFC and ADGM requirements.

This handbook provides a practical, business-focused overview of the UAE PDPL and its Executive Regulations, supporting organisations in building effective and sustainable data privacy programmes aligned with UAE regulatory expectations. The Executive Regulations provide additional clarity on how organisations should operationalise compliance with the law.

It is intended for business leaders, legal and compliance teams, data management, technology leaders and risk professionals who are responsible for how personal data is collected, used, shared and protected across the organisation.

In addition to data privacy, this handbook recognises the increasing use of data-driven and AI-enabled technologies in the UAE. Where relevant, responsible AI considerations are included to help organisations manage privacy, security and governance risks associated with AI, in line with the UAE National AI Strategy and the National Artificial Intelligence Security Policy.

The guidance in this handbook reflects UAE laws and regulations, as well as leading practices, and is designed to be practical, proportionate and scalable, enabling organisations to adapt it to their size, sector and risk profile.

# Data privacy & AI governance

## Brief introduction to key concepts

# A brief introduction

## Data privacy

Data privacy means giving people clear understanding and control over what personal data is collected about them, how it is used, and how it is protected, in line with the UAE Personal Data Protection Law (PDPL). It goes beyond information security, requiring organisations to process personal data lawfully, fairly, transparently, and accountably.

The UAE PDPL applies broadly to organisations operating in, or targeting, the UAE. It sets clear obligations for organisations and enforceable rights for individuals.

## Responsible AI

As organisations adopt data-driven technologies, including AI, strong data privacy governance becomes critical. While AI is not the primary focus of the law, its use can increase privacy, ethical, and operational risks if personal data is processed without appropriate controls and effective human oversight, and must therefore be implemented securely, fairly, and responsibly in line with UAE laws and national priorities that support trust in the digital economy.

In this handbook, responsible AI is positioned as a natural extension of UAE PDPL principles, helping organisations use data and AI.

## UAE Data Protection Law

In November 2021, the UAE issued Federal Law No. 45 of 2021 (the UAE Data Protection Law), with stricter standards for the protection of personal data and introduced clear obligations for organisations processing personal data in the UAE. The Law strengthens transparency, accountability and individuals' rights, and serves as a foundational pillar for trust in the UAE's digital economy. Compliance with the UAE PDPL is a core business responsibility for all organisations operating in or targeting the UAE.

## UAE National AI Strategy 2031 and AI Security Policy

The UAE National AI Strategy 2031 sets out the country's ambition to be a global leader in AI, leveraging AI to drive economic growth, innovation and government efficiency.
Complementing this ambition, the National Artificial Intelligence Security Policy of 2025 from the Cyber Security Council establishes expectations for the secure, controlled and trustworthy deployment of AI systems, with a focus on risk management, human oversight and protection against misuse.

# Why is data privacy and AI governance important?

Data privacy and AI governance are no longer compliance checkboxes – they are foundations of trust in a digital economy. As organizations increasingly rely on data and AI to drive decisions, automate processes, and innovate, the question is no longer *"Can we use this technology?"* but *"Can we use it responsibly, securely, and with confidence?"*

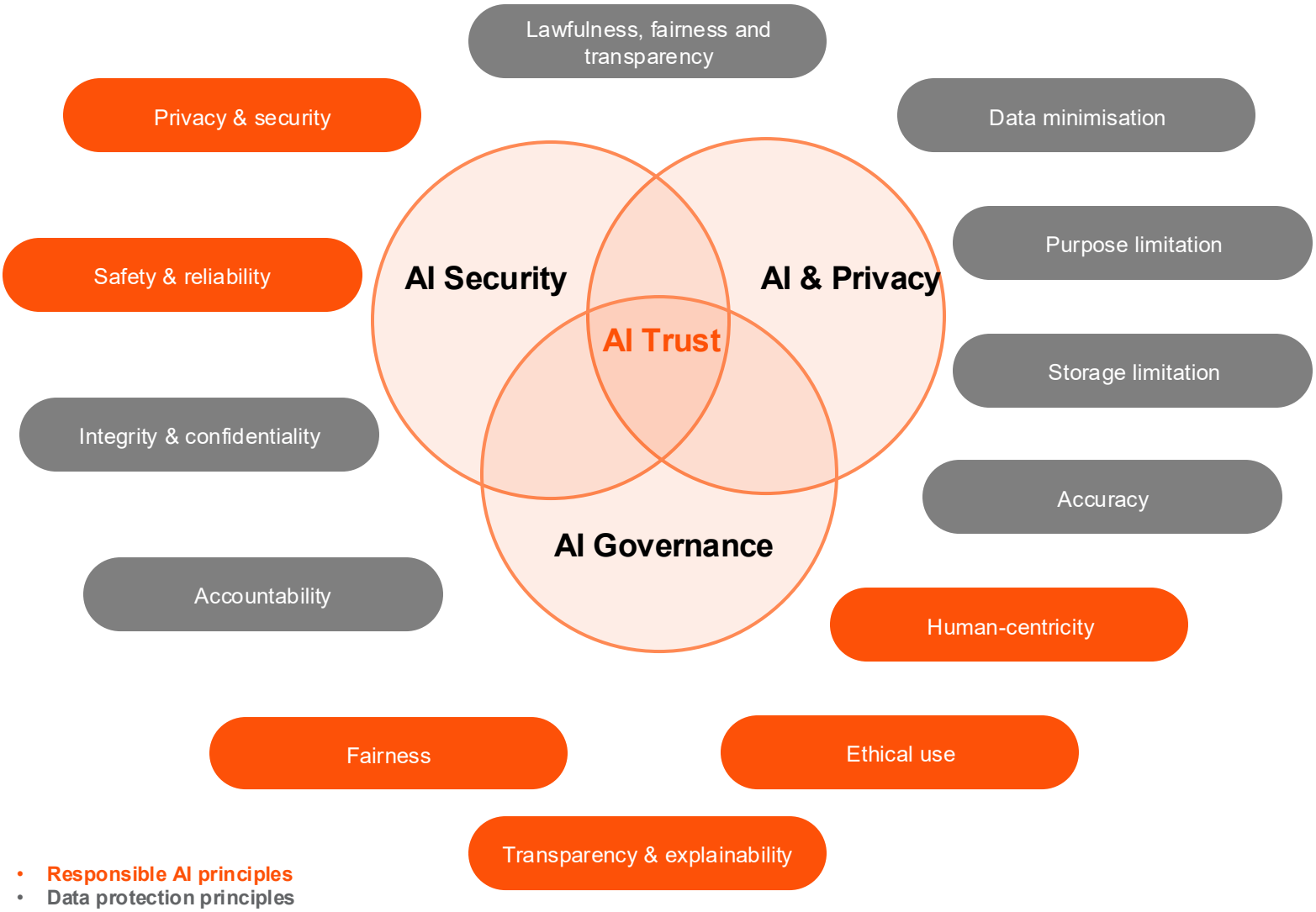
## Where AI and Privacy intersect

AI and privacy intersect at the point of data use. AI systems are trained, powered, and improved using vast amounts of data – often personal, sensitive, or business-critical. Decisions made by AI can directly impact individuals, organizations, and society.

## Trust is built through systems and people

Trust does not happen by accident. It is built through:

- Well-governed systems that embed privacy, security, and ethics by design
- Clear accountability for AI
- Skilled people who understand both the technology and its risks




- **Responsible AI principles**
- **Data protection principles**

# Examples of fines for non-compliance

## Case: Clearview AI (2024)

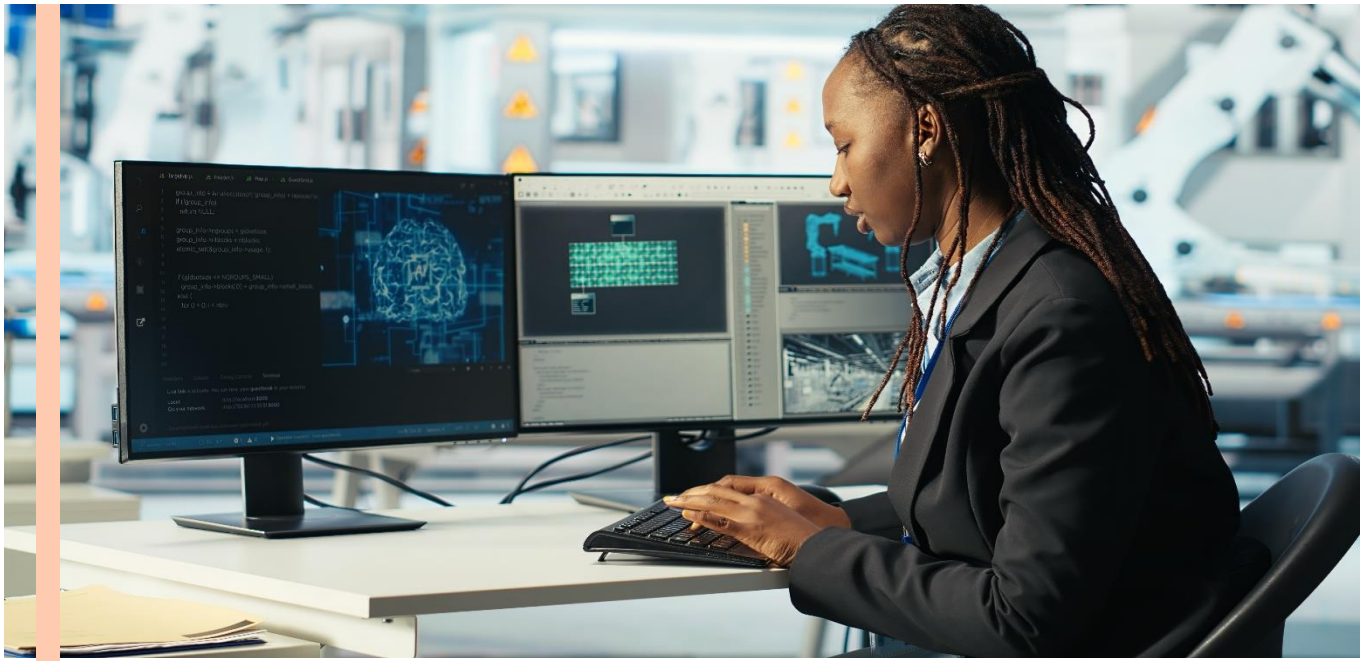
**Fine: €30.5 million** (~US $33.7 million)
**What happened:** The Dutch Data Protection Authority fined Clearview AI for building an illegal facial recognition database by scraping billions of photos and processing biometric data without a legal basis, violating multiple GDPR provisions.
**AI involvement:** AI facial recognition model used to identify individuals from scraped images.

## Case: OpenAI (2024)

**Fine:** €15 million (~US $16.3 million)
**What happened:** The Italian Data Protection Authority (Garante) fined OpenAI for unlawful processing of personal data in connection with ChatGPT, citing lack of a valid legal basis, insufficient transparency with regards to how personal data are collected and used (including for model training), inadequate age-verification measures for minors, and failure to promptly notify a data breach, in violation of multiple GDPR provisions.
**AI involvement:** Generative AI large language model trained and continuously improved using large-scale personal data and user interactions.

## Case: TikTok (2023)

**Fine: €345 million (**~US $368 million)
**What happened:** TikTok used AI-driven recommendation and profiling systems to analyse user behaviour and target content, including for children, without adequate transparency and privacy-by-design safeguards.
**AI involvement:** AI recommendation and profiling algorithms were central to the processing activity.



# What is personal data?

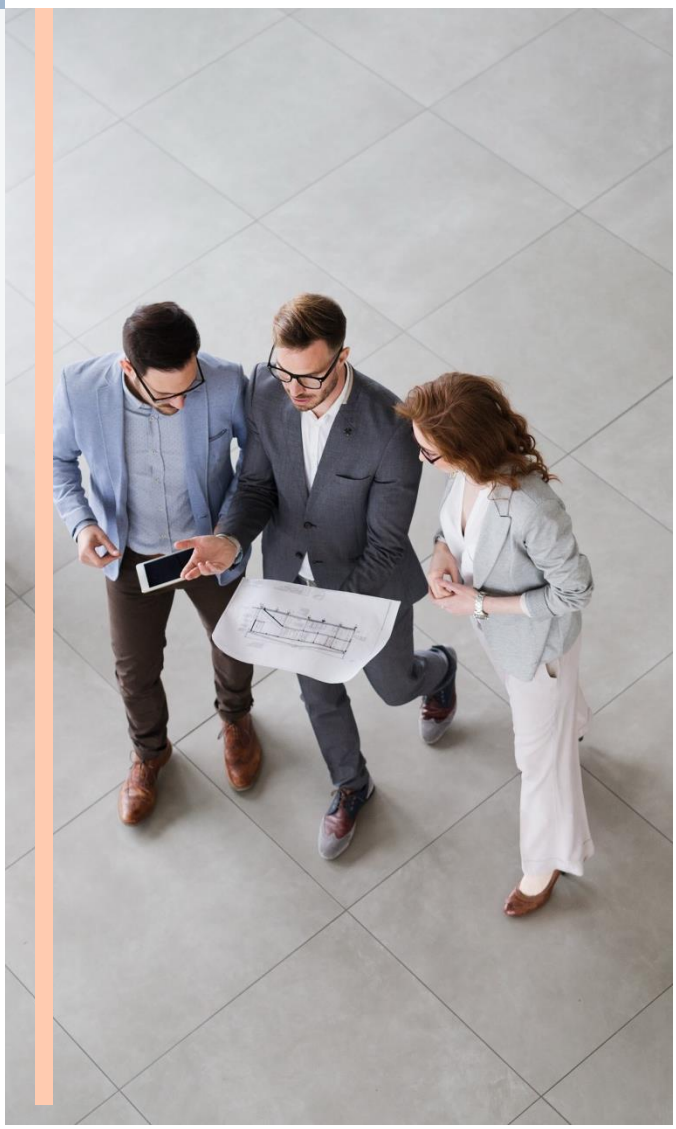
Personal data is any information that can identify either a living person, either directly or indirectly. This could be as simple as a name or account number or could be a digital identifier such as IP address, username or location data such as GPS coordinates.

## 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
- 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'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, license plate number

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.

# What is sensitive personal data?

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.

# People's (data subjects) 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 correct

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

### 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 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. The individual has the right to request 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 you process personal data?

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.

Identifying and documenting the applicable lawful basis is a key requirement when deploying AI systems that process personal data.

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 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.

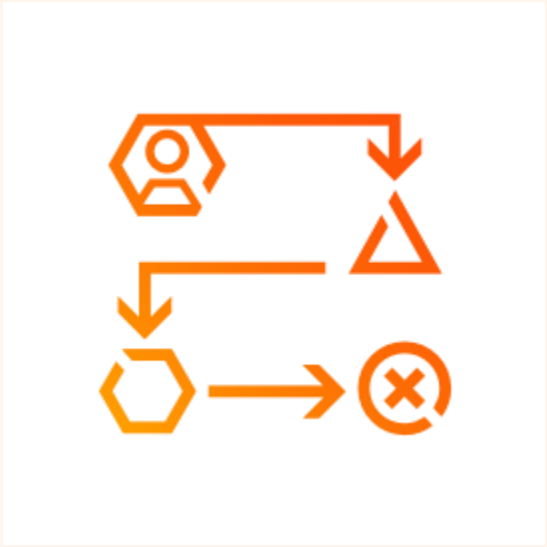
## Am I a data controller or a data processor?

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.

Contact your DPO or PwC to help you to determine the controller vs processor relationship.

# Ten steps to an effective data

## Privacy programme



# Ten steps to an effective data

## Privacy programme

**1**

Appoint a Data Protection Officer, where applicable

**2**

Maintain a personal data register

**3**

Ensure transparency and seek consent

**4**

Manage individuals' rights requests

**5**

Identify and enforce security mechanisms

**6**

Embed data privacy into your systems, processes and services

**7**

Handle personal data breaches

**8**

Manage third parties

**9**

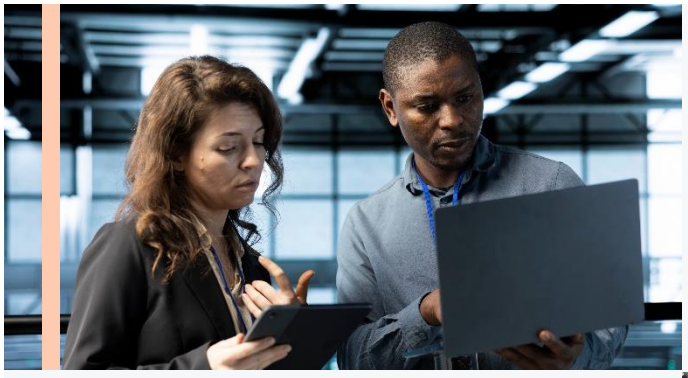
Control risks regarding cross-border data transfers

**10**

Operationalise Data Protection Programme, including training for all staff

# 1 Appoint a Data Protection Officer

The UAE Data Protection Law introduces the concept of a 'Data Protection Officer' (DPO), a leadership role for overseeing the organisation's data protection programme and ensuring compliance with applicable data protection laws.



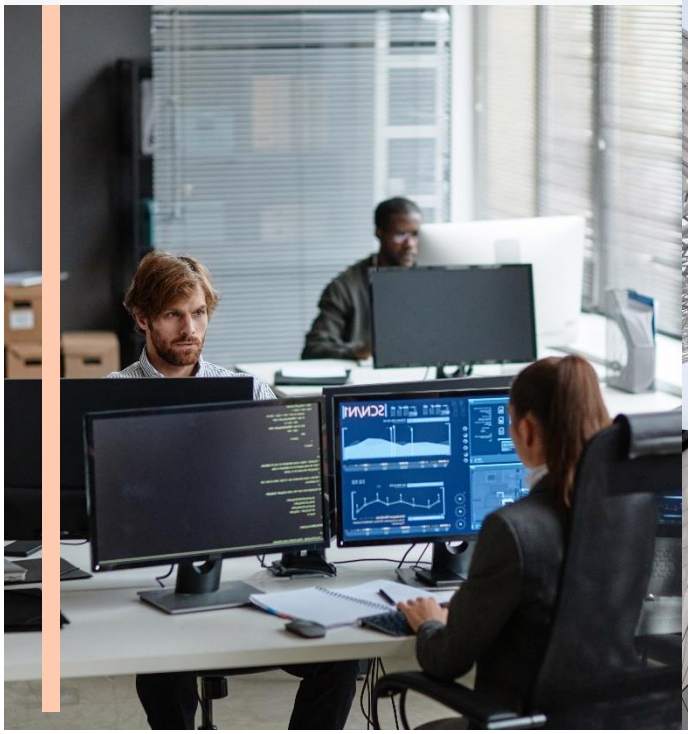
## What's the role of the appointed individual?

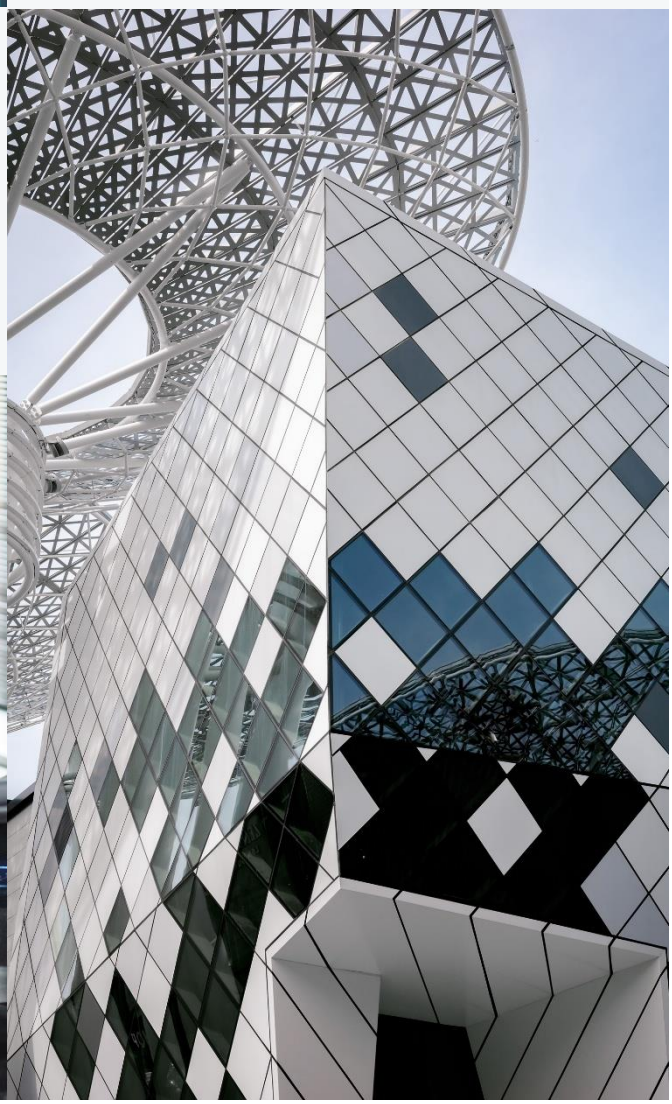
The appointed individual will assist you in monitoring internal compliance with the UAE Data Protection Law, advising you on your data protection obligations, providing expert advice when needed, and acting as a point of contact for individuals and data protection authorities.

## Who could act as an appointed individual?

The appointed individual can be an existing employees 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

To protect personal data you need to know, for example, 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 a personal data register, or what is often called a **'Record of Processing Activities' or 'RoPA'**. This is a requirement for both data controllers and data processors.

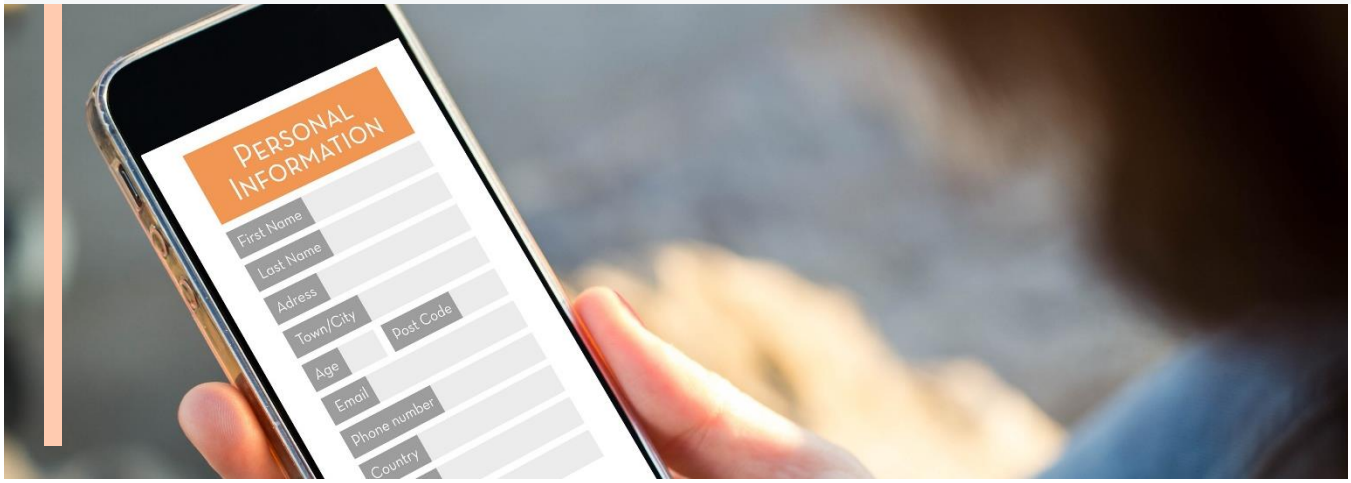
## How can I identify personal data being processed?

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 Ensure transparency 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 be provided to individuals?

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 transfer

## 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 their consent.

Consent means giving people control and choice over how their 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 any time, and the withdrawal procedures should be as easy as those for giving the consent.

# 4 Manage individuals' rights requests

## What are Data Subject Requests (DSRs)?

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. The data controller shall carry out the request for a personal data subject **within 30 days of receiving the request.**

## 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
- 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?

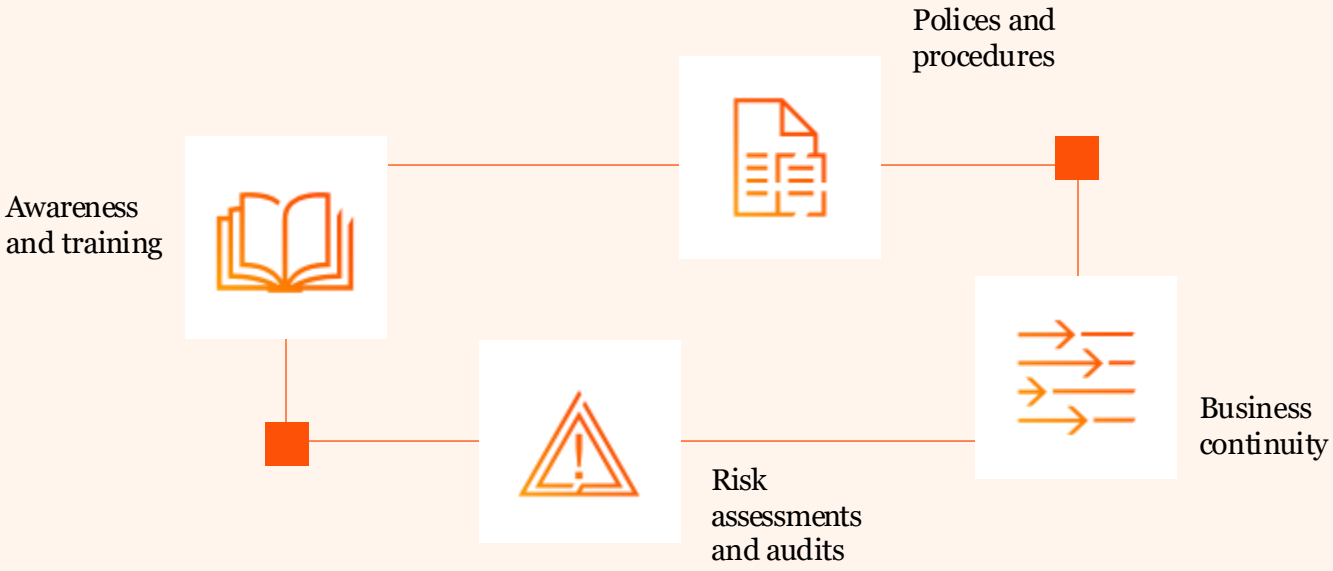
- Receive the data subject request and forward it to the concerned department
- Determine if the request is self-raised or on behalf of others, then verify the identity of the individual
- Determine where the personal data of the individual is stored, be it in systems or physical documents
- Perform the appropriate action according to the type of data subject request (i.e. copy data, delete data, restrict processing, etc.)
- Provide appropriate details to the DPO for delivery and response to the data subject
- 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 needs 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

# 6 Privacy by design & by default

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 Handle personal 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 notify The Office (the regulator) no later than 72 hours 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 immediately notify the data subject.

## How do I respond to a data breach?

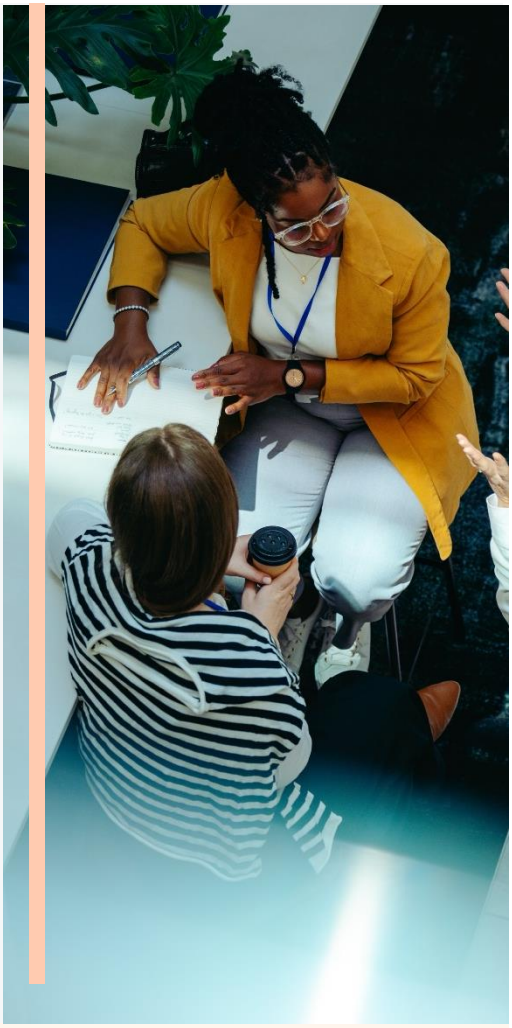
Once a data breach has been discovered, you must:

- 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

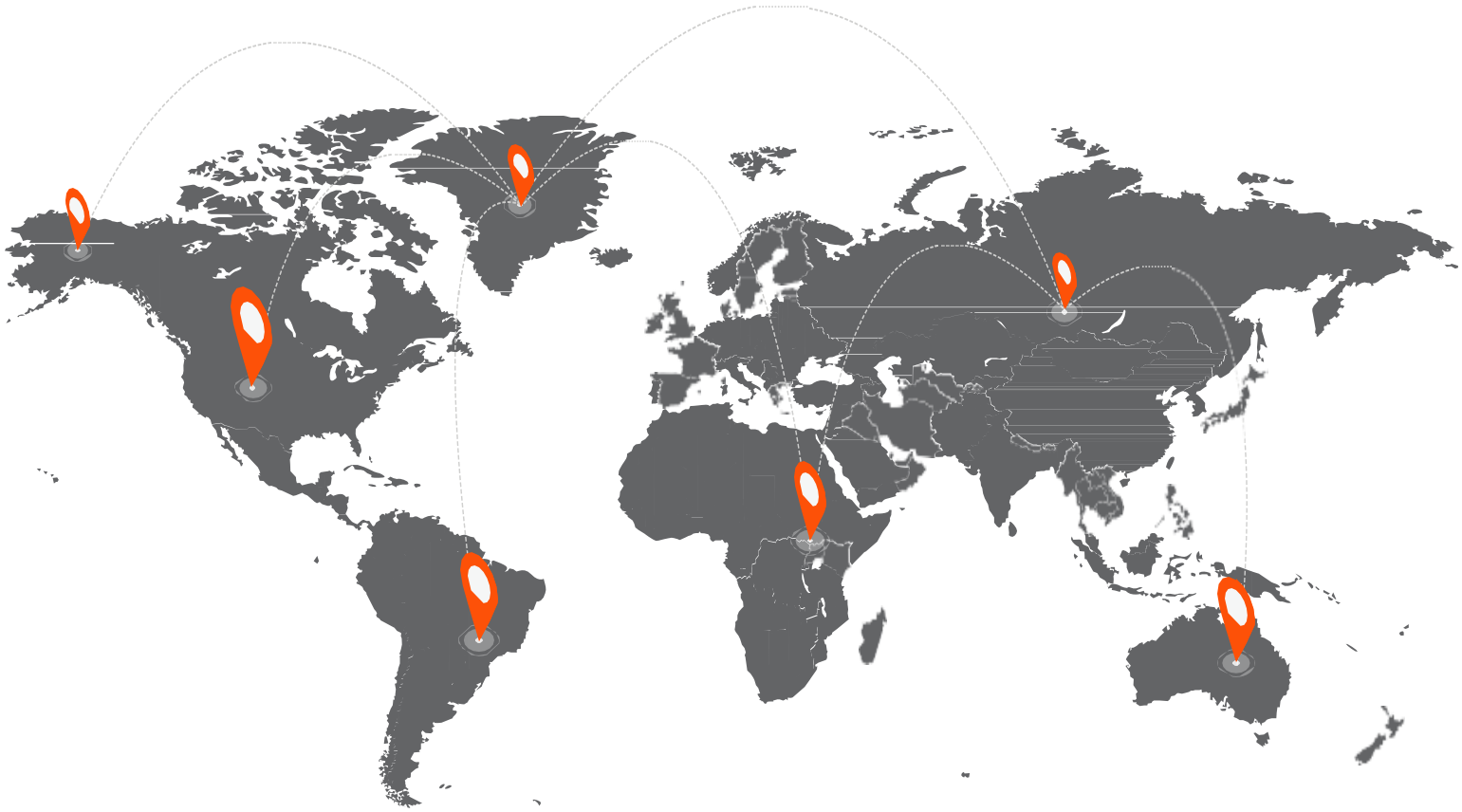
# 9 Control risks regarding cross-border data transfers

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 is expected to be issued by The office.

If the country is not in the 'whitelist', the company must conduct a potential risk and impact assessmentwhich shall take into consideration whether the recipient would provide a sufficient level of protection to the rights of the data subjects based on Artide 29 of the Executive Regulations.



## 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.

## What appropriate safeguards can be used if the country is not in the 'whitelist'?

The Executive Regulations include appropriate safeguards to protect personal data and the rights of personal data subjects.

- Standard contractual clauses
- Binding internal common rules
- Codes of conduct
- Accreditation certificates

**Public entities, being controllers or processors, shall sign a binding agreement for transfer of personal data.**

# 10 Operationalise Data Protection Programme, including training for all staff

Organisations shall operationalise its Data Protection Programme to ensure effective and ongoing compliance with the UAE PDPL. The program shall be embedded into business operations, governance structures, and decision-making processes to ensure that personal data is processed lawfully, fairly, and securely.

The Data Protection Programme shall include documented policies and procedures, defined roles and responsibilities, oversight mechanisms, and controls to support privacy-by-design and privacy-by-default across all processing activities.

Mandatory data protection training shall be provided to all staff, including partners, employees, contractors, and temporary personnel. Training shall be delivered at onboarding and refreshed periodically.

## Recommended content for a data privacy training

| | | |
|---|---|---|
| UAE PDPL overview, key requirements | Principles of personal data processing | Lawful basis for personal data processing |
| Data subjects' rights | Conducting risk assessments | Third party risk management |
| Cross-border data transfers | Data breach notification | Security of personal data |

# 9 steps to AI Privacy

## Governance for enterprises

**75%**
of employees in GCC have used AI tools in their roles over the past year *(vs 69% globally)*

**32%**
of employees in the region use GenAI tools daily *(vs 28% globally)*

**93%**
of CEOs predict AI will be integrated into tech platforms *(vs 78% globally)*

**90%**
of CEOs expect AI to enhance business processes and workflows *(vs. 76% globally)*

**81%**
of CEOs anticipate AI use in new product and service development *(vs. 63% globally)*

AI adoption is accelerating faster than organisations' ability to secure, govern and control it. As AI becomes operational, the primary risk is no longer whether organisations adopt AI. It is whether they remain in control of it.

## AI privacy framework

1. **AI privacy governance & strategy**
Establish clear accountability, principles, and oversight within AI Management System (AIMS) to ensure AI systems process personal data in compliance with applicable privacy laws.

2. **AI use cases & data inventory**
Maintain an up-to-date inventory of AI use cases and clearly document the personal data used across the AI lifecycle, including training, testing, deployment, inference, and outputs.

3. **Lawful basis & purpose limitation**
Ensure every AI use case has a documented lawful basis and that personal data is used strictly for defined, legitimate purposes throughout the lifecycle of the AI system.

4. **AI Privacy Risk and Impact Assessments (AI-DPIA)**
Identify, assess, and mitigate AI-specific privacy risks – such as profiling, automated decision-making – using a risk-based approach prior to deployment and during operation, with documented mitigation measures.

5. **Privacy by design & by default**
Embed data minimization, privacy-enhancing technologies, and protective controls into AI systems from design through deployment, operation, and change, in line with lifecycle and control requirements.

6. **Individual rights in AI**
Enable data subjects to exercise their privacy rights and ensure appropriate transparency, explainability, and human oversight in AI-driven decisions.

7. **Third-party & vendor AI privacy**
Manage privacy risks arising from AI vendors and service providers through due diligence, contractual safeguards, clearly defined responsibilities, and ongoing monitoring across the AI supply chain.

8. **Monitoring & incident management**
Continuously monitor AI systems for risks affecting personal data and ensure corrective actions in line with UAE PDPL breach notification requirements.

9. **Training & awareness**
Build organizational awareness and capability to use AI responsibly through targeted.

https://www.pwc.com/m1/en/media-centre/2025/hopes-and-fears-2025.html

# What you need to do – key steps

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.

**Records of processing activities / AI use cases inventory**

**What is provided**

- Stakeholder engagement and communications plan
- Personal data / AI use cases inventory
- Data flow maps showing the movement of personal data from collection through to disposal

**Gap assessment and roadmap**

**What is provided**

- Gap assessment report
- Roadmap with actionable recommendations based on identified gaps

**Strategy and target operating model**

**What is provided**

- Data privacy strategy (vision, mission, initiatives)
- Target operating model to ensure roles and responsibilities, KPIs are in place

**Data privacy / AI privacy programme implementation**

**Areas of focus**

- Governance and strategy
- Policy management
- Data lifecycle management
- Individual rights processing
- Risk management & compliance
- Privacy incident management
- Third party risk management
- Data security
- Training and awareness

**Ongoing operations and monitoring**

**What is provided**

- 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.


**Mona Maamer**
Partner, Cybersecurity &
Digital Trust Leader, PwC Middle East
+971 50 858 7380
mona.m.maamer@pwc.com

**Marea O'Toole**
Director, Cybersecurity &
Digital Trust, PwC Middle East
+971-50-406-9045
marea.otoole@pwc.com

**Ekaterina Volkovich**
Senior Manager, Cybersecurity &
Digital Trust, PwC Middle East
+971-50-938-6507
ekaterina.volkovich@pwc.com


At PwC, we help clients build trust and reinvent so they can turn complexity into competitive advantage. We're a tech-forward, people-empowered network with more than 370,000 people in 149 countries. Across audit and assurance, tax and legal, deals and consulting we help build, accelerate and sustain momentum. Find out more at www.pwc.com.

With over 12,000 people across 12 countries in 30 offices, PwC Middle East combines deep regional insight with global expertise to help clients solve complex problems, drive transformation, and achieve sustained outcomes. Learn more at www.pwc.com/me.