Data Privacy & Responsible AI Handbook for the Kingdom of Saudi Arabia

2026



About this handbook

We prepared this handbook to explain the key requirements of the Personal Data Protection Law (PDPL) of the Kingdom of Saudi Arabia (KSA) and help organisations to launch and strengthen their data privacy compliance programmed.

The handbook is designed for business leaders, legal and compliance experts, data management teams, technology and risk management professionals who are responsible for ensuring compliant and effective collection, usage and protection of personal data across their organisations.

In addition to data privacy, this handbook addresses the use of responsible AI in the KSA.

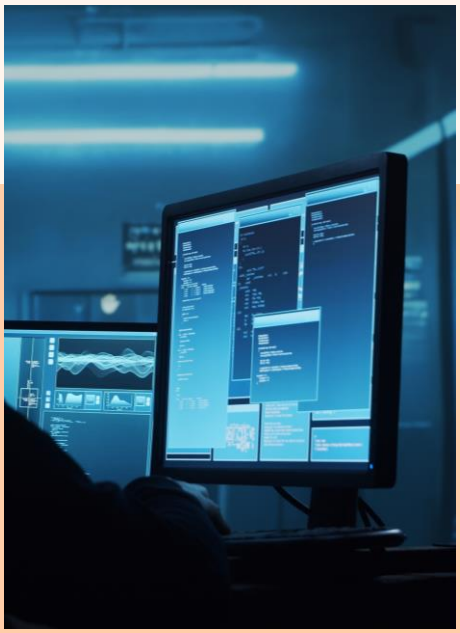
The guidance in this handbook is based on KSA regulatory rules, as well as best practices which we have observed.



Key concepts



Key concepts

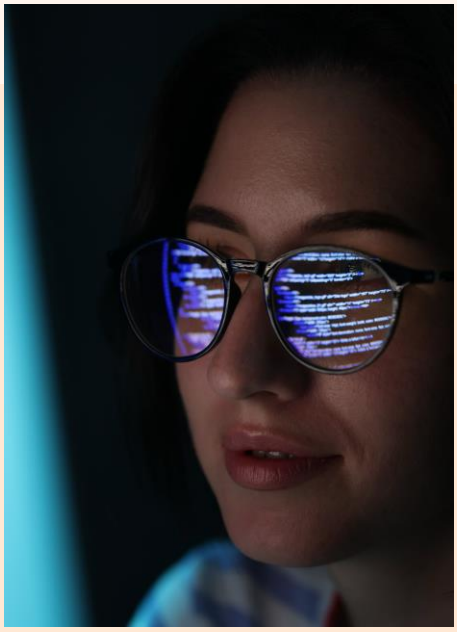


01

Data Privacy

Privacy, in its broadest sense, is a person's ability to keep others from intruding into their private sphere communications, and information about them. Personal data protection is one part of that broader concept. It means that personal data must be handled lawfully, fairly and transparently, and that the person has certain rights in relation to that data[1].

02



Responsible AI

Responsible AI is a set of practices that help organisations unlock the full potential of AI while addressing its inherent risks. These practices support a consistent, transparent and accountable approach to managing both risk and reward. They also ensure collaboration across stakeholders, helping shape strategies and policies that put effective risk management first, and maintain AI systems that reflect the organisation's values and objectives[2].

1. PwC analysis based on the KSA Personal Data Protection Law and international privacy principles.
2. https://www.pwc.com/gx/en/1/services/ai/responsible-ai.html

Key Concepts

03 Personal Data

Personal data is any data, regardless of its source or form, that may lead to identifying an individual specifically, or that may directly or indirectly make it possible to identify an individual[3].

Examples: Name, phone number, username, location data.

04 Sensitive Data

Sensitive data includes health data, racial or ethnic origin, or religious, intellectual or political belief, data relating to security criminal convictions and offences, biometric or genetic data and data that indicates that one or both of the individual's parents are unknown[4].

Examples: Sick leave information of employees; purchase history of drugs.



08 Processor

A processor is any public entity, natural person or private legal person that processes personal data for the benefit and on behalf of the controller[8].

Example: A cloud service provider or IT services provider gets access to the data of its client. The client will be a controller and the service provider – a processor.



05 Data Processing

Data processing includes any operation carried out on personal data by any means[5].

Examples: Storing of personal data in electronic systems; analyzing customers' preferences.

06 Data Subjects

Data subjects are individuals to whom the personal data relates[6].

Examples: Employees, customers.

07 Controller

A controller is a public entity, natural person or private legal person that specifies the purpose and manner of processing personal data, whether the data is processed by that Controller or by the processor[7].

Example: An employer that decides why and how employee data is used for payroll and HR records.



3. Article 1(4) of the KSA Personal Data Protection Law
4. Article 1(11) of the KSA Personal Data Protection Law
5. Article 1(5) of the KSA Personal Data Protection Law
6. Article 1(16) of the KSA Personal Data Protection Law
7. Article 1(18) of the KSA Personal Data Protection Law
8. Article 1(19) of the KSA Personal Data Protection Law

Why compliance matters: enforcement and penalties

Organisations face legal and financial exposure for non-compliance with the PDPL.

The enforcement landscape in 2026

Full enforcement in effect

The PDPL and its Implementing Regulations are fully enforceable as of 2026, with no further grace period for organisations operating in the Kingdom.

Administrative fines

General PDPL and Implementing Regulation violations can attract warnings or administrative fines of up to SAR 5 million, and fines may be doubled for repeat offences[9].

Criminal sanctions

Disclosing or publishing sensitive personal data with intent to harm a data subject or achieve a personal benefit can lead to up to 2 years of imprisonment[10].

An active regulator

SDAIA has demonstrated an active enforcement approach under the PDPL, issuing enforcement decisions against non-compliant organisations while continuing to supervise data controllers, investigate complaints and violations; and require corrective actions to strengthen compliance[11].

Common violations

Examples of violations include[12]:

- Sending marketing messages without recipient's proper consent
- Missing the 72-hour deadline to report a breach to SDAIA
- Not appointing a Data Protection Officer when the PDPL required one
- Not putting the right organisational measures in place to protect data subjects' rights.

Extraterritorial reach

The PDPL also applies to organisations outside the Kingdom that process the personal data of individuals residing in Saudi Arabia[13].

9. Article 36 of the KSA Personal Data Protection Law
10. Article 35 of the KSA Personal Data Protection Law
11. https://www.spa.gov.sa/en/N2489505
12. https://www.spa.gov.sa/en/N2489505
13. Article 2 of the KSA Personal Data Protection Law

What's changed since the PDPL came into force?

The PDPL and its Implementing Regulations are fully enforceable. All organisations dealing with personal data must comply with them.

From transition period to active supervision

Full enforcement

The transition period ended on 14 September 2024, making the PDPL and its Implementing Regulations fully enforceable from that date[14].

Enforcement architecture

SDAIA is obliged to establish committees to review violations of the PDPL and its Implementing Regulations[15].

Transfer rules in force

SDAIA issued the Regulation on Personal Data Transfer Outside the Kingdom[16], establishing detailed requirements for cross-border transfers, including adequacy assessments, approved transfer safeguards and transfer risk assessments.

New SDAIA rules and guidance

SDAIA has issued rules[17] and guidance covering Data Protection Officer's appointment, controller's registration, privacy policies, records of processing activities, breach incidents and related compliance topics.

Marketing consent focus

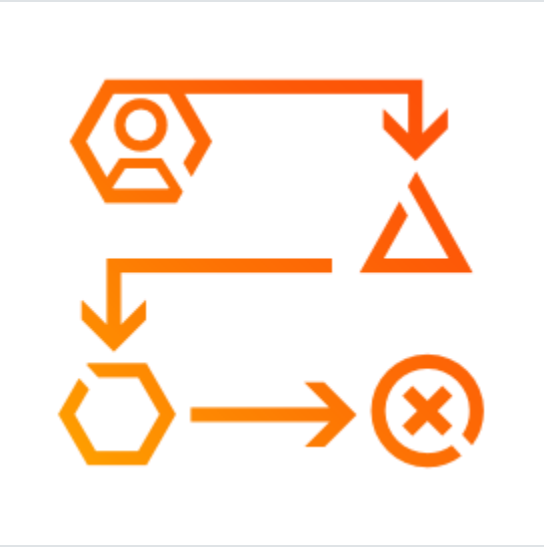
As a general rules PDPL requires consent for direct marketing and advertising or awareness messages[18].

AI documents

SDAIA has issued the AI Adoption Framework[19].

14. https://dgp.sdaia.gov.sa/wps/portal/pdp/knowledgecenter/details/PDPLCP/%21ut/p/z0/04_Sj9CPykssy0xPLMnMz0vMAfljo8ziPR1dzTwMgw2MDMOcTA3MjH39TE29jY0MQsz1g1Pz9L30o_ArAppiVOTr7JuuH1WQWJKhm5mXlq8fEeAS4OMcoF-Q7R4OAFcDiug%21/
15. Article 36 of the KSA Personal Data Protection Law
16. https://sdaia.gov.sa/Documents/RegulationonPersonalDataEN.pdf
17. https://sdaia.gov.sa/en/SDAIA/about/Documents/RulesforAppointingPersonalDataProtectionOfficer.pdf
18. Article 25 of the KSA Personal Data Protection Law, Articles 28 and 29 of the Implementing Regulation to the PDPL
19. https://sdaia.gov.sa/en/SDAIA/about/Files/AIAdoptionFramework.pdf,

Controller registration & DPO



Two foundational obligations: Registration and the DPO appointment

In the beginning of your privacy compliance journey, ask yourself who will manage the data protection programme. It is recommended to appoint a Data Protection Officer (DPO) to manage day-to-day activities. For some organisations, the DPO appointment is mandatory under the Implementing Regulation and SDAIA DPO rules.

Controller registration and the Data Protection Officer (DPO)



01

Register as a controller

Controllers may be required to register on the national platform maintained by SDAIA, recording who they are and how they process personal data[20].

How to register

Registration is completed through SDAIA's national data governance platform, with the information kept current as processing activities change.

Why it matters

Registration supports transparency and supervision, and failing to register is among the violations the regulator actively monitors.



02

When a DPO is required

SDAIA Rules for Appointing Personal Data Protection Officer[21] require a DPO for public entities providing large-scale personal-data services, controllers whose core activities involve large-scale regular monitoring, and controllers whose core activities involve sensitive data. That said, it is recommended to have a responsible individual to manage data protection whether required or not.

Who can serve as DPO

The DPO may be an official, employee or external contractor, with the expertise and resources needed to monitor PDPL compliance.

DPO responsibilities

The DPO monitors compliance, supervises impact assessments and audits, enables data subject rights, acts as the SDAIA contact point, and supports breach notifications and Records of Processing (RoPA) updates, as well answering employee questions about data protection and providing ongoing trainings.

20. https://dgp.sdaia.gov.sa/wps/wcm/connect/047a4149-ba11-4919-9341-260164125ba5/The+Rules+Governing+the+National+Register+of+Controllers+Within+the+Kingdom.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=ROOTWORKSPACE-047a4149-ba11-4919-9341-260164125ba5-q1h55or

21. https://sdaia.gov.sa/en/SDAIA/about/Documents/RulesforAppointingPersonalDataProtectionOfficer.pdf

Ten steps to personal data protection compliance



Ten steps to personal data protection compliance

01 **Records of processing activities (RoPA)**
Map what personal data is processed, why it is used, where it flows, who receives it, how long it is retained and what controls protect it.



02 **Lawful bases for processing**
Confirm and document the lawful basis for each processing activity, including consent, actual interest, legal requirement or previous agreement, public entity security or judicial purposes, or legitimate interest where permitted.



03 **Data protection impact assessment (DPIA)**
Identify high-risk processing and document privacy risks, mitigations, approvals and follow-up actions before deployment or material change.



04 **Security of personal data**
Apply proportionate organisational, administrative and technical controls, including access management, encryption, monitoring, secure deletion and incident readiness.



05 **Data privacy notices**
Provide clear notices explaining purposes, lawful basis, categories of data, recipients, retention, rights and contact channels.



06 **Data subject rights**
Enable individuals to submit, track and receive timely responses to rights requests and maintain an auditable request register.



07 **Personal data breach notification**
Maintain breach detection, escalation and notification procedures to assess whether SDAIA and affected individuals must be notified.



08 **Contracting processors**
Perform due diligence, define roles, put Article 17 processor terms in place and monitor processors throughout the relationship.



09 **Cross-border data transfers**
Identify transfers, assess the transfer basis, apply adequacy, approved safeguards or limited exemptions, and limit transfers to the minimum personal data necessary.



10 **Policies and procedures**
Adopt, communicate and periodically refresh policies that operationalise privacy governance, accountability and day-to-day compliance.

01 Records of processing activities (RoPA)

Records of Processing Activities (RoPA) are basically the backbone of all data protection programmed. Why? This is the information that tells us what personal data is collected, where it is stored, if we share the data, if an assessment needs to be performed, among other activities. The RoPA must be accurate, up to date and available to SDAIA on request.

Under the Implementing Regulation, your RoPA records should be retained during the processing period and for five years after the activity ends[22].

Examples of the details which should be included in the RoPA[23]

- Description of processing activities performed by the organisation.
- Purpose of each processing activity.
- Categories of personal data and data subjects involved in each processing activity.
- Lawful bases for processing activities.
- The expected period for which personal data shall be retained.
- Technical and organisational measures applied to protection of personal data.
- The entities with which personal data could be shared.
- Whether personal data is transferred outside the KSA, including transfer legal basis and recipients.
- Controller contact details and Data Protection Officer details, where required.

SDAIA has created a helpful guideline regarding how to manage RoPAs[24].

Note: Structure the RoPA in such a way, so it shows personal data processing details in relation to each business unit of your organisation. SDAIA's sample RoPA shown below for illustration:

SDAIA

Field	Description
Controller Name	Specify the Controller name and relevant contact details.
Personal Data Protection Officer Details	Fill in the details related to the personal data protection officer, in the cases requiring its appointment.
Processing Activity	Detailed identification of all personal data processing activities aligned with the Controller's operations and activities. This includes categorizing datasets containing personal data and classifying internal activities that directly handle personal data.
Activity Description	A comprehensive description of each personal data processing activity that provides sufficient detail to understand the impact and associated risks of the activity.
Activity Start Date	Commencement date of the personal data processing activity.
Activity End Date	Date of data destruction and deletion of personal data processing activities records, as the case may be.
Business Unit	Name of the business unit responsible for processing activities.
Processing Purpose	Clearly and precisely identifying the purpose for processing personal data. For example: Marketing or recruitment.
Legal Basis	The legal basis to justify the specified purpose of processing personal data.
Personal Data Subject Categories	Description of the personal data subject categories whose data is being processed. Examples: Employees, clients, members.
Processed Personal Data Categories	Description of the personal data categories being processed. Examples: Contact details, location, health data, credit data.
Personal Dataset Names	Specifying names for the personal datasets.
Personal Datasets Owner	Specifying the individual(s) who own the personal datasets.
Personal Datasets Tool / Location	The tool(s) containing the personal datasets being processed or their storage locations.

Note: Each processing activity identified requires a lawful basis

22. Article 33 of the Implementing Regulation to the PDPL
23. Article 31 of the KSA Personal Data Protection Law, Article 33 of the Implementing Regulation to the PDPL
24. https://sdaia.gov.sa/Documents/PersonalDataProcessingActivitiesRecordsGuideline.pdf

02 Legal bases for processing

A legal basis is a lawful justification for using personal data. Without a correct legal basis, you may not process personal data. See below examples of the key legal bases specified in the PDPL, from which you must choose the most appropriate ones.

The appropriate legal bases can be found in the KSA PDPL with the Implementing Regulation providing further detail.

Examples of lawful bases[25]

Consent

> Example of a processing activity: Sending direct marketing materials to an individual.

Legitimate interest of the controller (if data is not sensitive)

> Example of a processing activity: Fraud detection or network security.

Previous agreement with the data subject

> Example of a processing activity: Delivering a product to an individual using the address they provided.

Actual interest

> Example of a processing activity: Urgent medical support where contacting the individual is impossible or difficult.

Requirements of the law

> Example of a processing activity: Retaining employee payroll or tax records where required by law.

Public entity's security purposes or judicial requirements

> Example of a processing activity: Processing CCTV or access logs by a public entity for security purposes.

Note: After identifying the appropriate lawful basis for processing, ensure that you comply with the specific regulatory requirements associated with that basis.

Example 1: Consent

The consent must be obtained, documented and managed in accordance with Articles 11 and 12 of the PDPL Implementing Regulations[26]. In addition, explicit consent is required where the processing involves sensitive data, credit data or decisions based solely on automated processing.

Example 2: Legitimate interests

The controller must conduct and document a legitimate interest assessment in accordance with Article 16 of the Implementing Regulations[27].

Please refer to the KSA PDPL and its Implementing Regulations.

25. Articles 5 and 6 of the KSA Personal Data Protection Law
26. Articles 11 and 12 of the Implementing Regulation to the PDPL
27. Articles 16 of the Implementing Regulation to the PDPL

03 Data protection impact assessment (DPIA)

Once you have identified all your processing activities and documented them in the Records of Processing Activities (RoPA), you need to identify which activities require a data protection impact assessment (DPIA), which effectively assess any risks of the personal data and describes how such risks could be mitigated.

Examples below:

	Processing activity requiring DPIA[28]	Example
1	Processing of sensitive data	Managing health data of employees
2	Collecting, comparing, or linking two or more sets of personal data obtained from different sources	Evaluation of an employee based on several databases
3	Continuous and large-scale processing of personal data of those who fully or partially lack legal capacity	Extensive analysis of children data
4	Processing operations that require continuous monitoring of data subjects	Operation of the CCTV in premises
5	Processing personal data using new technologies	Application of AI in data analysis
6	Making decisions based on automated processing of personal data	Operating an automated decision-making system to decide whether to grant financing
7	Providing a product or service that involves processing personal data that is likely to cause serious harm to the privacy of data subjects	Using facial-recognition payment systems

Note: Document the DPIA in a form of a written report. Assign a responsible person who will be in charge of implementing recommendations to mitigate the risks revealed by the DPIA.

28. Article 25 of the Implementing Regulation to the PDPL

04 Security of personal data

Organisations are required to take necessary organisational, administrative and technical measures to protect personal data[29]. That said, the law does not prescribe specific techniques, organisations themselves must choose the measures that are the most suitable for their processing activities.

Examples of the measures to protect personal data:

Organisational measures

Implement instruments on responding to data subject's requests	Managing access to the systems processing personal data	Performing ongoing personal data protection compliance monitoring	Providing training to the personnel on the topics of personal data protection

Administrative measures

Assigning the responsibility for protection of personal data to specific employees	Approve and maintain data protection policies and procedures	Conduct and document data protection impact assessments	Keeping and maintaining the RoPA up-to-date

Technical measures

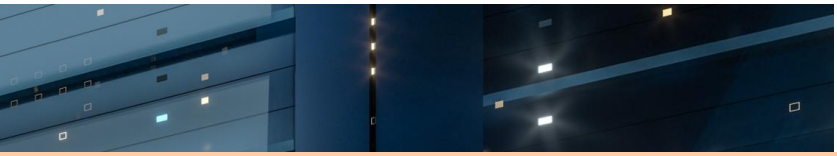
Encryption in transit and at rest	Pseudonymisation / anonymisation	Secure deletion / destruction controls	Having in place technical capability to detect, contain, and evidence a breach

Note: Pay additional attention to those processing activities that involve health data and credit data. These activities are subject to additional requirements of the PDPL and Implementing Regulation.

29. Article 19 of the KSA Personal Data Protection Law

05 Data privacy notices

Organisations must be transparent about how they process personal data. This is achieved by publishing privacy notices (also called privacy policies and privacy statements), so that data subjects can understand how their personal data is being used (processed) and protected.

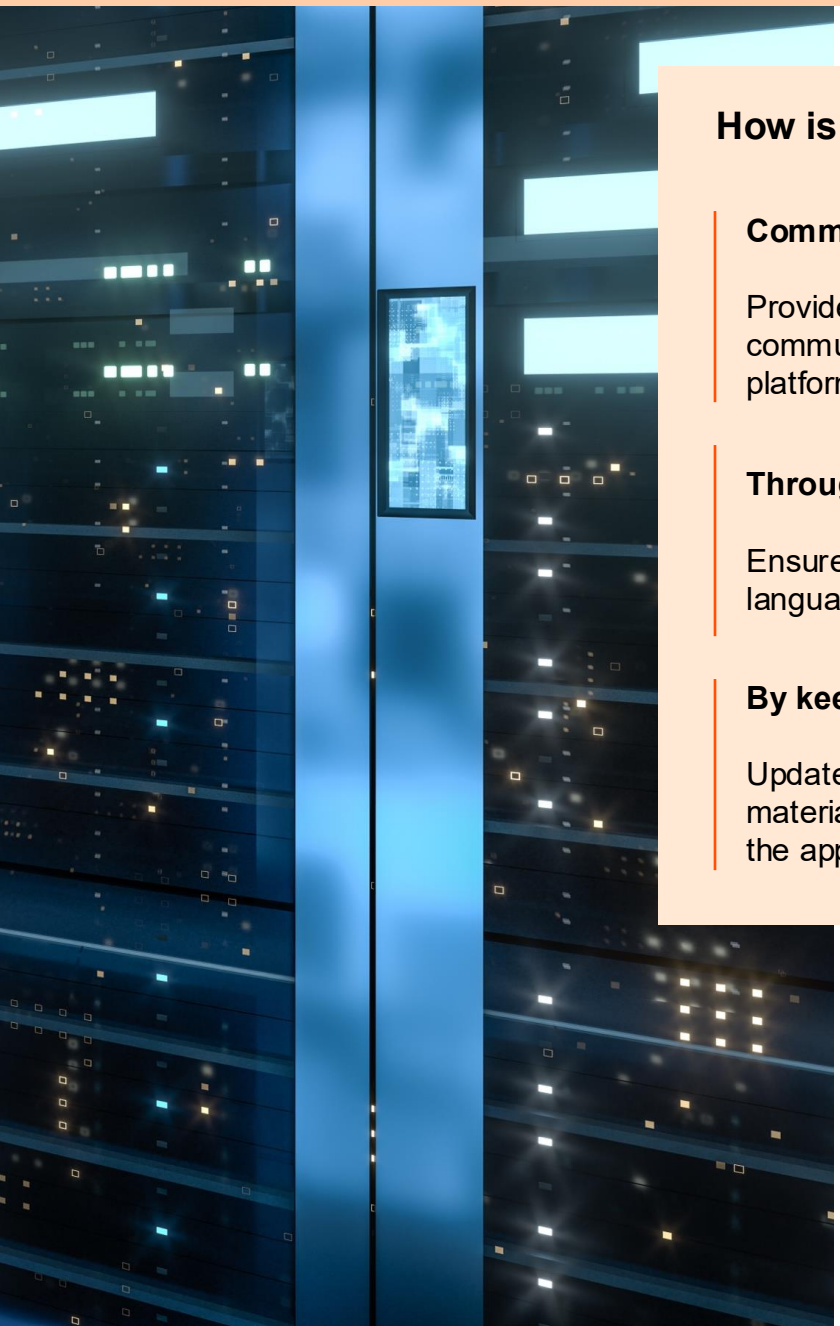


When is the privacy notice provided?[30]

Before or at the time of collection, when collecting directly from the data subject.

Within 30 days, if personal data is collected not directly from the data subject.

Before any further processing for a new purpose beyond the original one.



How is the privacy notice provided?

Communication channels

Provide the privacy notice through adequate communication channels – e.g., website, online platforms, applications.

Through clarity

Ensure the privacy notice is written in a clear language that the data subject can understand.

By keeping it up-to-date

Update the privacy notice if processing activities materially change (e.g., the purposes have changed, the approach to retention periods has changed, etc.).

Note: Use completed Records of Processing Activities as a tool to develop privacy notices. Take from it all necessary information about your personal data processing activities and outline this information in privacy notices in a clear and simple way.

30. Article 4 of the Implementing Regulation to the PDPL

06 Data subject rights

Every individual has certain rights under PDPL[31] in relation to their personal data. Organisations that process personal data must ensure that individuals can exercise these rights in an effective way.

01

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 of such a collection.

02

Right to access personal data

Individuals have the right to access their personal data.

03

Right to request a copy of personal data

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

04

Right to request correction

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

05

Right to destruction

Individuals can request destruction (erasure) of their personal data.

The actions required by the data subject's right request must be performed **within 30 days**. This timeline may be extended for an **additional 30 days** in exceptional circumstances[32] (response requires unpredictable or unusual additional efforts, receipt of multiple requests from the same data subject).



Maintain a register where all requests on data subjects' rights and responses to them shall be recorded.

Note: Consider establishing a single preference centre, that will provide individuals with functionality to submit data subject rights requests in a convenient way.

31. Article 4 of the KSA Personal Data Protection Law
32. Article 4 of the Implementing Regulation to the PDPL

07 Personal data breach notification

Organisations must assess every personal data breach and notify SDAIA within 72 hours where it may harm personal data or the data subject, or conflict with data subject rights or interests. Affected data subjects must be notified without undue delay where required[33].

Notifying data subjects

The controller shall notify data subjects without undue delay if the breach may damage their data or conflict with their rights or interests.

Notify data subjects via email, text messages or – if a large group of data subjects is affected – via website, social media or other appropriate means.

Notifying SDAIA

The controller shall notify SDAIA within 72 hours of becoming aware of a Personal Data Breach if it may harm personal data or the data subject, or conflict with the data subject's rights or interests.

Notify SDAIA of the personal data breach via **National Data Governance Platform.** If the platform is not available, send a notification via email and save the email that was sent.



Note: Have in place a detailed data breach response policy that will describe in which cases a breach can be considered as causing damage to personal data or conflict with data subjects' rights or interests. It will help you to decide whether a breach requires a notfication to SDAIA and/or data subjects.

33. Article 24 of the Implementing Regulation to the PDPL

08 Contracting processors

Organisations may cooperate only with processors that provide sufficient guarantees to protect personal data and comply with the PDPL and its Implementing Regulation[34].

Key rules when engaging a processor

01 Define the role

Before drafting a processor agreement, clearly understand the role of the counterparty. Is it a processor or another controller?

02 Due diligence

Require the processor to provide evidence that it properly protects personal data, such as policies, certifications and control reports.

03 Prepare the data processing agreement

When drafting the processing agreement, specify roles, purpose, data categories, duration, breach notification, sub-processors and other Article 17 terms.

04 Determine rights and obligations

Specify in detail what exactly each counterparty shall be doing. For instance, how the parties will cooperate if either receives a data subject rights request, etc.

05 Update the privacy notice and RoPA

Ensure that your RoPA and privacy notices specify the processors with whom you share personal data.

06 Ongoing monitoring

Regularly require the processor to provide evidence that personal data remains duly protected.

Note: As soon as possible, review existing processor agreements against Article 17 of the Implementing Regulation and update documents where needed.

34. Article 8 of the KSA Personal Data Protection Law, Article 17 of the Implementing Regulation to the PDPL

09 Cross-border data transfers

Cross-border transfers move personal data from Saudi Arabia to recipients abroad. They are permitted subject to compliance with the requirements of Article 29 of the PDPL[35] and SDAIA Regulation on Personal Data Transfer Outside the Kingdom[36].

Examples of activities that include cross-border data transfers

01 Transmission

Data is transmitted to any entity located outside the KSA

02 Remote Access

Data stored in the KSA is accessed by employees, contractors, or service providers outside the KSA

03 Temporary Sharing

Data is temporary shared with a third party located outside the KSA for analysis, reporting, or technical support

04 Payment Operations

Data is processed by an international payment processor, financial institution, or vendor located outside the KSA

05 Merger and Acquisition

Data is transferred as part of a merger, acquisition, or partnership where a non-KSA entity gains access to the data

06 Tangible Medium Transportation

Data is stored on a tangible medium (e.g. laptop, smartphone, paper documents, etc.) the medium is transferred outside the KSA

Key documents often required for a lawful cross-border data transfer

Records of Processing Activities (RoPA)	Standard Contractual Clauses (SCCs)	Binding Common Rules (BCRs)	Transfer Assessment Report (TIA)
Identify in the RoPA the processing activities involving transfer of personal data outside the KSA.	Use SDAIA-approved Standard Contractual Clauses.	Use Binding Common Rules prepared in accordance with SDAIA requirements for eligible intra-group transfers.	Conduct a Transfer Risk Assessment where required and document it in a report.

35. Article 4 of the KSA Personal Data Protection Law

36. SDAIA Regulation on Personal Data Transfer Outside the Kingdom

10 Policies and procedures

It is highly recommendable that every organisation adopts policies and procedures that translate PDPL obligations into internal rules for protecting personal data. These documents help employees understand what is required and provide evidence of governance, accountability and compliance.

The law does not prescribe specific types of policies and procedures to be in place. Based on our experience the following documents are highly useful:

Data protection framework policy

The document describes the key features of the personal data protection function - including its structure and its responsibilities.

Data subject requests procedure

The document describes how to respond to the requests from the data subjects, including describing the channels used to communicate with them.

Consent management policy

The document describes how to collect consent for processing of personal data, what are the requirements to consent and how the withdrawal of consent is managed.

Personal data breach response procedure

The document describes how the employees must cooperate in case of the breach of personal data.

Third party policy

The document describes how to onboard and monitor processors and other entities that process personal data of the organisation.

Data protection impact assessment procedure

The document describes how to assess personal data protection risks, where required by PDPL and Implementing Regulation.

Data retention policy

The document describes how to determine retention periods for the personal data.

Cross-border data protection policy

The document describes how to manage transfers of personal data from KSA to another country.

Artificial intelligence governance policy

The document describes how to assess personal data protection risks, where required by PDPL and Implementing Regulation.

Note: Provide employees with regular training on how policies and procedures should be implemented.

Sovereignty, residency & localisation

Additional PDPL concepts and baseline accountability obligations



Data sovereignty, residency and localisation

These three terms are often used interchangeably, but they mean different things and carry different implications under the Kingdom's data rules.

Three related but distinct concepts

Data sovereignty	Data residency	Data localisation
The principle that data is ultimately subject to the laws and regulators of the country where it sits in the Kingdom, that means the PDPL, SDAIA, and NDMO.	Where data is normally stored or processed. Data may sit in a defined location yet still be mirrored or backed up elsewhere under agreed controls.	A stricter requirement that specific datasets must physically remain in-country, with transfers abroad allowed only under narrow, defined exceptions.
The PDPL applies extraterritorially, so personal data about Saudi residents stays within its reach even when hosted or processed abroad.	Cross-border transfers are allowed where an adequacy decision applies (pending publication), or under approved safeguards,	Government, critical, and certain regulated datasets may be required to stay in-country.

Note: Classify your data first. Knowing which datasets are sensitive, regulated, or government-related tells you whether localisation applies or whether a controlled cross-border transfer is enough.

Responsible AI



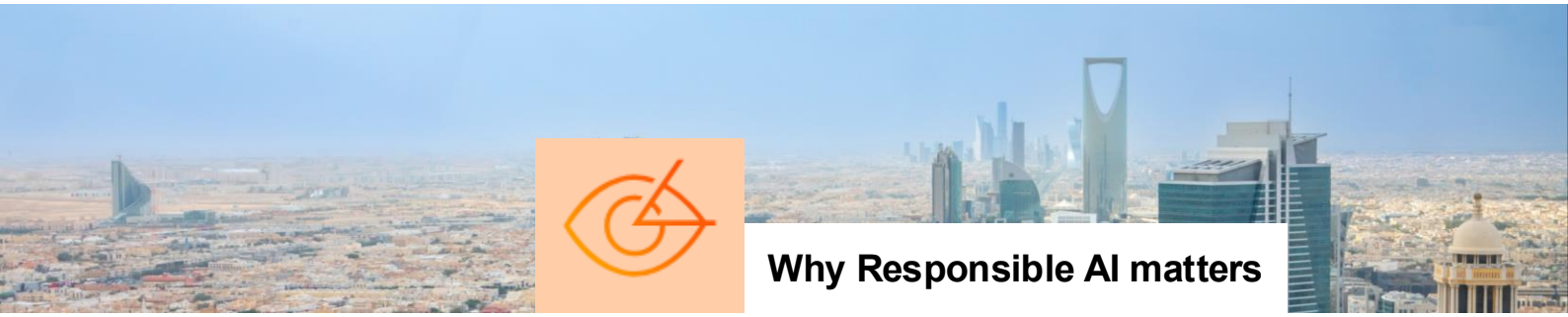
Responsible AI in the Kingdom of Saudi Arabia

Source: PwC Analysis

Artificial Intelligence is becoming embedded into business processes, customer services, decision-making, analytics, automation, and digital transformation programmed across the Kingdom of Saudi Arabia. As AI adoption accelerates, organisations must ensure that AI systems are not only innovative and efficient, but also lawful, ethical, secure, explainable, fair, and subject to appropriate human oversight.

Responsible AI refers to the governance, risk management, controls, and operating practices that enable organisations to design, develop, procure, deploy, and monitor AI systems in a way that protects individuals, supports organisational objectives, and aligns with KSA regulatory expectations, SDAIA AI Ethics Principles, PDPL requirements, cybersecurity controls, and recognised international standards.

Responsible AI should be embedded across the full AI lifecycle and integrated into existing governance, privacy, cybersecurity, risk, data management, procurement, legal, compliance, and internal audit processes.



Why Responsible AI matters

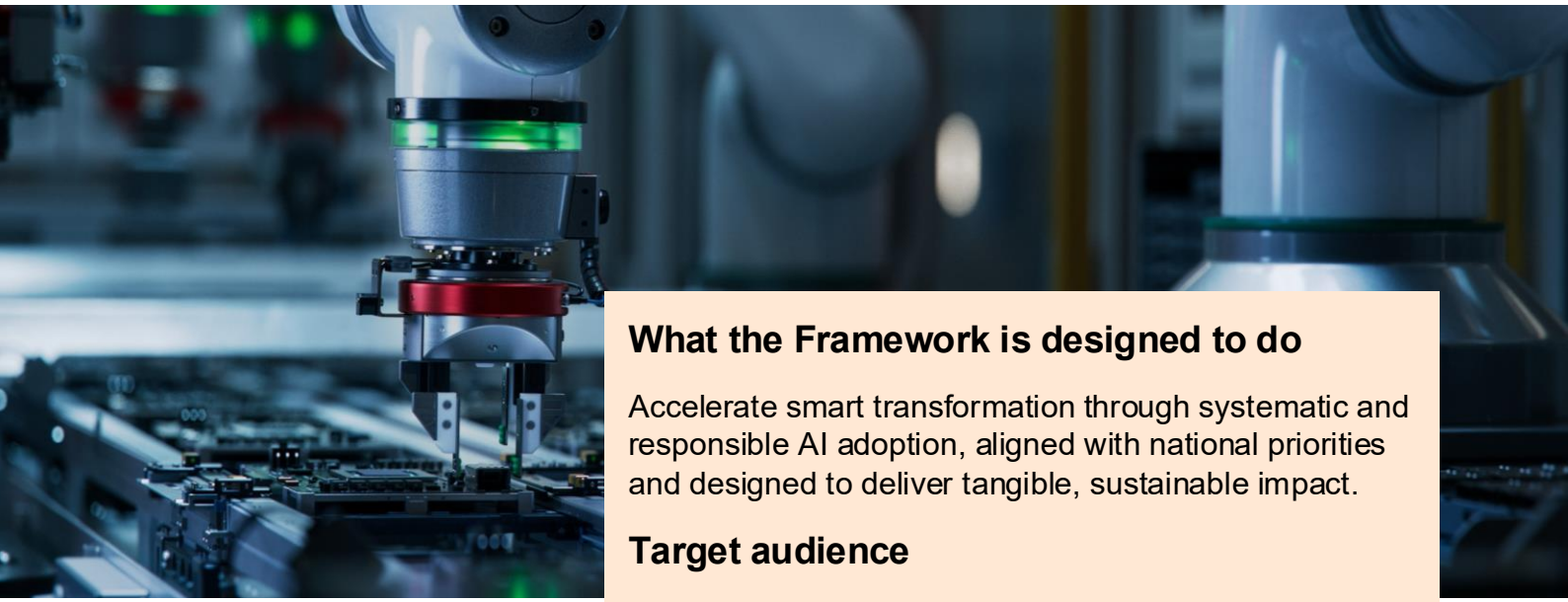
AI systems can create significant value by improving productivity, decision-making, customer experience, operational efficiency, and innovation. However, they can also introduce new and amplified risks, including:

- Unfair or biased outcomes;
- Lack of explainability or transparency;
- Inaccurate, misleading, or unsafe outputs;
- Unlawful or excessive use of personal data;
- Automated decisions affecting individuals;
- Security vulnerabilities and data leakage;
- Uncontrolled use of public GenAI tools;
- Third-party and cloud AI risks;
- Lack of accountability for AI outcomes;
- Reputational, regulatory, legal, and operational harm.

In KSA, responsible AI is particularly important because AI systems may interact with personal data, national data, government services, critical infrastructure, financial services, healthcare, education, transport, smart cities, and other priority sectors. Organisations should therefore apply a risk-based approach that reflects the nature, purpose, scale, data sensitivity, affected individuals, and potential impact of each AI use case.

SDAIA AI Adoption Framework

A practical reference for adopting AI responsibly across public and private sector organisations in the Kingdom.



What the Framework is designed to do

Accelerate smart transformation through systematic and responsible AI adoption, aligned with national priorities and designed to deliver tangible, sustainable impact.

Target audience

Government entities, private entities, policymakers and legislators seeking practical guidance for AI planning, implementation and evaluation.

How to use it

Use the Framework as a roadmap to assess maturity, establish the enabling environment, prioritise AI initiatives and strengthen governance for responsible AI.

Three interconnected pillars

Directions

It covers the strategic foundation for AI adoption, focusing on clear objectives, effective governance, well-designed AI initiatives and strong adherence to organisational policies and frameworks.

Enablers

It covers the foundational capabilities that support successful AI adoption, including skilled talent, high-quality and reliable data, and robust, scalable technology systems. They provide the infrastructure and resources needed to develop, operate and sustain AI solutions effectively.

Outcomes

AI adoption outcomes measure the real business value delivered by AI. They focus on how effectively AI models are developed and deployed, the strength of monitoring, security and governance controls, and the tangible benefits achieved.

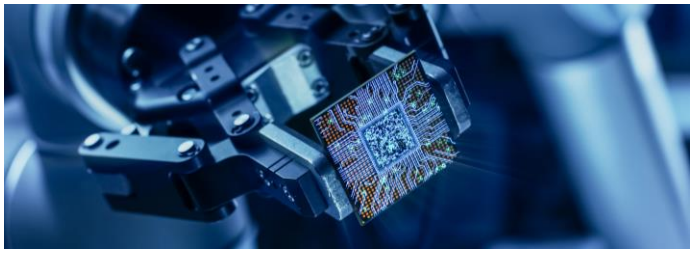
Key KSA responsible AI references (1/2)

Ten regulatory and governance reference points that shape responsible AI in the Kingdom of Saudi Arabia.

01 SDAIA AI Ethics Principles

Describes the ethical principles, risk categories, lifecycle expectations, and accountability requirements for the responsible design, development, deployment, and monitoring of AI systems in KSA.





02 KSA Personal Data Protection Law and Implementing Regulations

Sets the core legal requirements for processing personal data in KSA, including lawful basis, data subject rights, impact assessments, breach notification, and controller and processor obligations.

03 SDAIA Regulation on Personal Data Transfer outside the Kingdom

Define the rules, safeguards, assessments, and contractual requirements for transferring or accessing personal data outside KSA, including where AI systems or vendors involve cross-border processing.





04 National Data Governance Policies

Establish national expectations for managing data as an organisational asset, including data classification, ownership, quality, sharing, access, retention, and governance controls.

05 NCA Essential, Cloud and Data Cybersecurity Controls

Define baseline cybersecurity requirements for protecting systems, cloud environments, and data, including governance, access control, resilience, monitoring, and incident response.

Key KSA responsible AI references (2/2)

Ten regulatory and governance reference points that shape responsible AI in the Kingdom of Saudi Arabia.



06 Sector-specific regulatory requirements

Set additional obligations for specific sectors such as financial services, telecoms, healthcare, insurance, aviation, or government, where AI use may require enhanced oversight or approvals.

07 SDAIA Deepfakes Guidelines

Guidance on the responsible creation and use of synthetic and deepfake media, including disclosure, consent, and safeguards against deceptive or harmful AI-generated content.





08 SDAIA Generative AI Guidelines

Guidance for organisations and the public on adopting generative AI responsibly, covering acceptable use, data protection, human oversight, and risk considerations.

09 SDAIA AI Adoption Framework

Provides a comprehensive framework for the strategic, responsible and scalable adoption of AI in KSA; covering governance, capability development, implementation enablers, maturity assessment and performance outcomes aligned with national priorities.



10 NCA AI Cybersecurity Guidelines

Provides cybersecurity requirements and controls for the secure design, development, deployment, operation and monitoring of AI systems in KSA, covering cybersecurity governance, defence, resilience and third-party risk management to mitigate AI-related cybersecurity risks and strengthen organisational and national cyber resilience.

AI international best practice

Eight international standards and frameworks that anchor responsible AI.

1	**ISO/IEC 42001 - AI Management Systems**	International standard for establishing, operating, and continually improving an AI management system, covering governance, policies, roles, and lifecycle controls.
2	**ISO/IEC 23894 - AI Risk Management**	Guidance for identifying, assessing, and treating AI risks across the lifecycle.
3	**NIST AI Risk Management Framework**	Voluntary framework structured around the Govern, Map, Measure, and Manage functions to build and sustain trustworthy AI.
4	**EU AI Act**	Risk-based regulation setting obligations for prohibited, high-risk, and limited-risk AI, including transparency, human oversight, and conformity assessment.
5	**ISO/IEC 27001 - Information Security**	International standard for an information security management system protecting the confidentiality, integrity, and availability of information.
6	**ISO/IEC 27701 - Privacy Information**	Extension to ISO/IEC 27001 establishing a privacy information management system for processing personal data as a controller or processor.
7	**OWASP Top 10 for LLM Applications**	Community-driven list of the most critical security risks for large language model and generative AI applications, such as prompt injection and data leakage.
8	**OECD AI Principles**	Intergovernmental standard promoting trustworthy AI through human-centred values, transparency, robustness, accountability, and inclusive growth.

Responsible AI guiding principles (1/2)

We gathered key Responsible AI principles based on SDAIA requirements and international best practice. These principles provide a practical foundation for designing, deploying, and monitoring AI systems.

Responsible AI principle	Explanation	Reference to laws / standards
Fairness and non-discrimination	AI systems should be designed, tested, and monitored to avoid unfair bias, discrimination, or unjustified differential treatment of individuals or groups.	**SDAIA AI Ethics Principles** - fairness; **NIST AI RMF** - fair with harmful bias managed; **EU AI Act** - controls for certain high-risk and prohibited AI practices.
Privacy and data protection	Personal data used in AI systems should be processed lawfully, fairly, transparently, and securely, with data minimisation, purpose limitation, retention controls, DPIAs, privacy notices, and privacy by design.	**SDAIA AI Ethics Principles** - privacy and security; **KSA PDPL and Implementing Regulations** - lawful processing, transparency, DPIAs, rights, retention, security, and breach notification; **ISO/IEC 27701** - privacy information management; **NIST AI RMF** - privacy-enhanced AI.
Transparency and explainability	Individuals and stakeholders should be informed when AI is used in a meaningful way, and AI outcomes should be explainable to an appropriate level based on risk and context.	**SDAIA AI Ethics Principles** - transparency and explainability; **KSA PDPL and Implementing Regulations** - transparency and notice obligations; **NIST AI RMF** - accountable and transparent, explainable and interpretable; **EU AI Act** - transparency obligations for certain AI systems.
Human oversight	AI systems, especially higher-risk systems, should include appropriate human review, escalation, override, and appeal mechanisms.	**SDAIA AI Ethics Principles** – accountability and responsibility; **NIST AI RMF** - AI risk governance and management; **EU AI Act** - human oversight requirements for high-risk AI systems; **ISO/IEC 42001** - human oversight and lifecycle governance controls within an AI management system.

Responsible AI guiding principles (2/2)

We gathered key Responsible AI principles based on SDAIA requirements and international best practice. These principles provide a practical foundation for designing, deploying, and monitoring AI systems.

Responsible AI principle	Explanation	Reference to laws / standards
Accountability and responsibility	Clear ownership should be assigned for AI systems, including business owners, technical owners, data owners, risk owners, and control owners.	**SDAIA AI Ethics Principles** - accountability and responsibility; **ISO/IEC 42001** - AI management system, policies, roles, responsibilities, governance, and continual improvement; **NIST AI RMF** - Govern function and accountability structures.
Reliability, safety, and robustness	AI systems should be tested before deployment and monitored during operation to ensure they perform as intended, remain accurate, and do not create unacceptable risks.	**SDAIA AI Ethics Principles** - reliability and safety; **NIST AI RMF** - valid and reliable, safe, secure and resilient; **ISO/IEC 23894** - AI risk management; **EU AI Act** - accuracy, robustness, and cybersecurity requirements for high-risk AI systems.
Security and resilience	AI systems should be protected against cybersecurity threats, data leakage, model manipulation, prompt injection, adversarial attacks, unauthorised access, and third-party compromise.	**SDAIA AI Ethics Principles** - privacy and security; **NCA Essential Cybersecurity Controls, Cloud Cybersecurity Controls, and Data Cybersecurity Controls** - cybersecurity governance, protection, monitoring, and resilience; **ISO/IEC 27001** - information security management; **OWASP Top 10 for LLM Applications** - GenAI and LLM security risks.
Social and environmental benefit	AI should support legitimate business, public, and social value while avoiding harmful, deceptive, manipulative, or unsafe applications.	**SDAIA AI Ethics Principles** - social and environmental benefits and humanity; **NIST AI RMF** - management of risks to individuals, organisations, and society; **ISO/IEC 42001** - responsible development and use of AI systems, including governance and stakeholder impact considerations; **OECD AI Principles** - inclusive growth, sustainable development, and human well-being as foundations for trustworthy AI.

AI Privacy and Data Protection Requirements

Source: PwC Analysis

Data Privacy Compliance for AI



Where AI systems process personal data, organisations should apply the PDPL requirements across the AI lifecycle.

This includes:

- Documenting AI processing activities in the RoPA;
- Identifying lawful basis for AI-related processing;
- Conducting DPIAs where AI involves sensitive data, combining or linking data sets, large-scale monitoring, new technologies, automated decision-making, or activities likely to cause serious harm;
- Providing clear privacy notices;
- Enabling data subject rights;
- Applying data minimisation and retention controls;
- Protecting personal data through technical and organisational measures;
- Managing processor and vendor arrangements;
- Assessing cross-border transfers;
- Notifying SDAIA and affected individuals where reportable personal data breaches occur.

For higher-risk AI use cases, organisations should consider an AI-DPIA or combined AI impact assessment that covers both privacy and broader responsible AI risks, including fairness, explainability, human oversight, security, and operational impact.

GenAI and LLM governance



Generative AI and large language models require additional controls because they may generate inaccurate content, expose sensitive information, process prompts outside approved environments, or interact with tools and systems in unpredictable ways.

Organisations should establish specific GenAI rules covering:

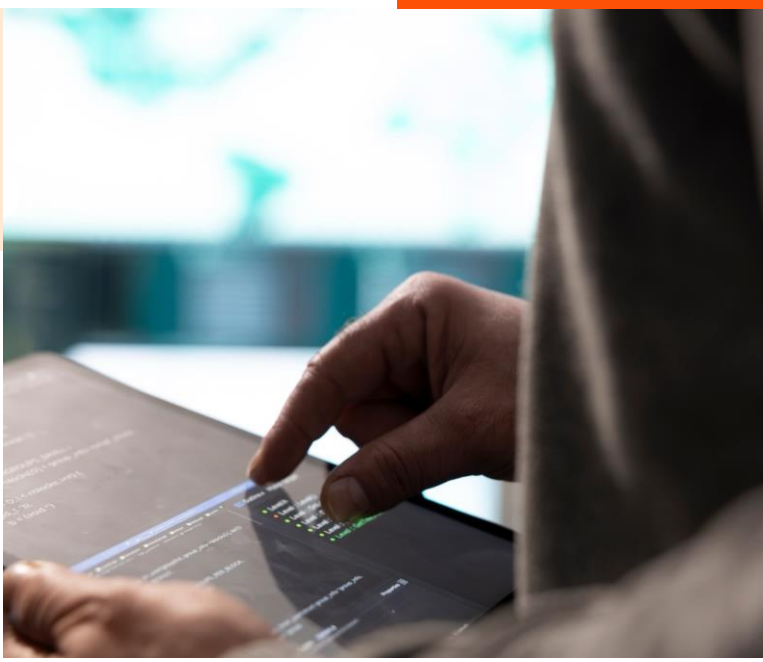
- Approved and prohibited GenAI tools;
- Restrictions on entering personal, confidential, client, government, or sensitive data into public AI tools;
- Prompt management and user guidance;
- Review of AI-generated outputs before use;
- Hallucination and accuracy checks;
- Copyright and intellectual property considerations;
- Secure use of retrieval augmented generation;
- Controls over plugins, agents, APIs, and tool access;
- Monitoring for prompt injection and data leakage;
- Retention and logging of prompts and outputs;
- Human accountability for final decisions and deliverables.

High-risk GenAI use cases should not be deployed without formal approval, documented testing, cybersecurity review, privacy assessment, and business owner sign-off.

AI Privacy Framework

Source: PwC Analysis

Nine building blocks for embedding privacy across the AI lifecycle.



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.

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.

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.

AI Privacy Risk and Impact Assessments (AI-DPIA)
Identify, assess, and mitigate AI-specific privacy risks – such as sensitive-data processing, dataset linking, continuous monitoring or automated decisions – before deployment and during operation, with documented mitigation measures.

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

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

Lawful basis & purpose limitation
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.

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

Training & awareness
Build organisational awareness and capability to use AI responsibly through targeted training programmed, role-specific guidance, and regular communication.

Organisations in KSA should align AI use with SDAIA AI Ethics Principles, PDPL requirements, national cybersecurity expectations, and leading international frameworks such as ISO/IEC 42001. By embedding governance, privacy, security, transparency, fairness, human oversight, and monitoring across the AI lifecycle, organisations can unlock the benefits of AI while maintaining trust, accountability, and regulatory readiness.

What you need to do

As experts in AI Governance and 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 Data Privacy and AI Governance programmed, with tools and accelerators to assist the process.

Records of processing activities/ AI 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
Data Privacy Gap assessment and roadmap / AIMS Gap Assessment	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 • Policy management • Data lifecycle management • Individual rights processing • Risk management & compliance (DPIA, AI risk & impact assessments, etc.) • 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



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



Shoaib Masood
Senior Manager, Cybersecurity &
Digital Trust, PwC Middle East
shoaib.s.masood@pwc.com



Edward Lewis
Manager, Cybersecurity &
Digital Trust, PwC Middle East
edward.l.lewis@pwc.com



Alexander Ladeyshchikov
Manager, Cybersecurity &
Digital Trust, PwC Middle East
alexander.ladeyshchikov@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.

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.

© 2026 PwC. All rights reserved