Data privacy & responsible AI handbook for Qatar

A guide based on the Qatari Data Protection

Table of contents

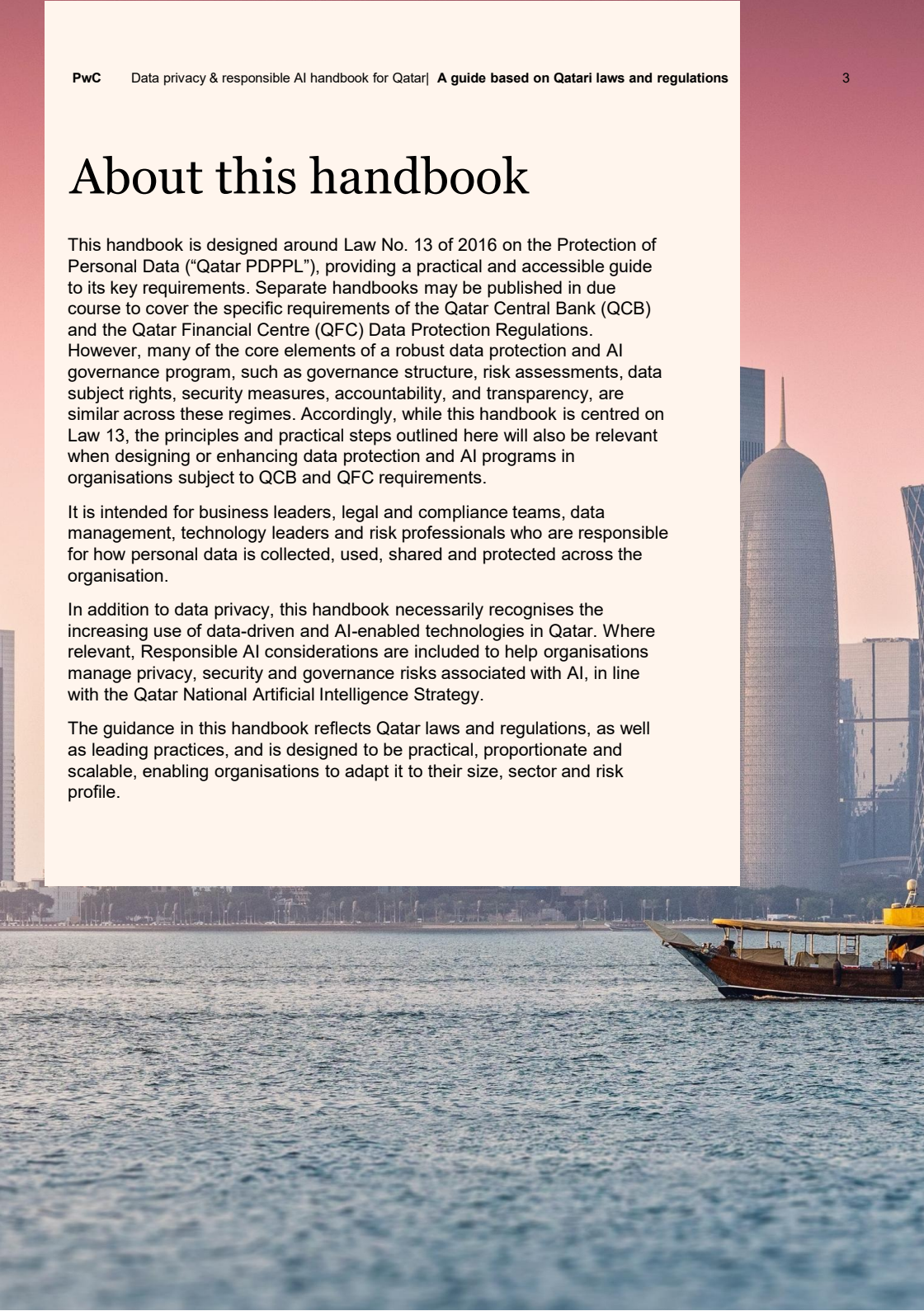
About this handbook

This handbook is designed around Law No. 13 of 2016 on the Protection of Personal Data ("Qatar PDPPL"), 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 Qatar Central Bank (QCB) and the Qatar Financial Centre (QFC) Data Protection Regulations. However, many of the 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 Law 13, the principles and practical steps outlined here will also be relevant when designing or enhancing data protection and AI programs in organisations subject to QCB and QFC requirements.

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 necessarily recognises the increasing use of data-driven and AI-enabled technologies in Qatar. Where relevant, Responsible AI considerations are included to help organisations manage privacy, security and governance risks associated with AI, in line with the Qatar National Artificial Intelligence Strategy.

The guidance in this handbook reflects Qatar 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.



01

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 applicable data privacy laws and regulations. It goes beyond information security, requiring organisations to process personal data lawfully, fairly, transparently, and accountably.

The Qatar PDPPL applies broadly to organisations operating in, or targeting, Qatar. It sets clear obligations for organisations and enforceable rights for individuals and is complemented by sector-specific regimes such as the QCB requirements and the QFC Data Protection Regulations.

Responsible AI

As organisations adopt data-driven technologies, including artificial intelligence (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 Qatari laws and national priorities that support trust in the digital economy.

In this handbook, Responsible AI is positioned as a natural extension of Qatar PDPPL principles, helping organisations use data and AI in compliance with the law.

While this handbook focuses on the PDPPL, it is useful to understand the wider Qatari framework, including QCB data protection requirements, QFC Data Protection Regulations, and the Qatar National AI Strategy (QNAIS):

Qatar Personal Data Privacy Protection Law (PDPPL)

Qatar's Personal Data Privacy Protection Law (Law No. 13 of 2016) establishes a comprehensive framework for the protection of personal data and regulates how organisations collect, process, store, and transfer personal data. The Law strengthens transparency, accountability, and individuals' rights, and serves as a foundational pillar for trust in Qatar's digital economy. Compliance with the PDPPL is a core responsibility for all organisations operating in or targeting Qatar.

Qatar Central Bank (QCB) Data Handling & Protection Regulations

The Qatar Central Bank (QCB) has issued data handling and protection regulations applicable to financial institutions under its supervision. These regulations introduce specific requirements for data governance, security controls, customer data protection, and operational resilience, and operate alongside the PDPPL to reinforce data privacy and security in the financial sector.

Qatar Financial Centre (QFC) Data Protection Regulations

The Qatar Financial Centre (QFC) Law provides a separate legal and regulatory framework for entities operating within the QFC. Organisations licensed by the QFC are subject to the QFC Data Protection Regulations, which set out requirements for lawful processing, data subject rights, security measures, and cross-border data transfers, aligned with international standards.

Compliance with the QFC data protection framework applies to activities conducted within the QFC.

Qatar National Artificial Intelligence Strategy

The Qatar National Artificial Intelligence Strategy sets out Qatar's ambition to leverage AI to drive economic diversification, innovation, and public sector transformation, in alignment with Qatar National Vision 2030. The strategy promotes responsible and ethical AI adoption, supported by strong data governance, privacy protection, and trust in AI systems.

The NCSA issues helpful guidance for organizations

The National Cyber Security Agency (NCSA) issues guidelines for regulated entities to support organisations in complying with the Qatar PDPPL. Key documents and tools include:

Booklets and Guidelines

1. PDPPL Guidance Booklet
2. Controller and Processor Guideline
3. Data Privacy by Design and by Default Guideline
4. Data Privacy Impact Assessment (DPIA) Guideline
5. Electronic Communications for Direct Marketing Guideline
6. Exemptions Applicable to Competent Authorities
7. Exemptions Applicable to Data Controllers
8. Individuals' Complaints Guideline
9. Individuals' Rights Guideline
10. Personal Data Breach Notifications Guideline
11. Personal Data Management Systems (PDMS) Checklist
12. Principles of Data Privacy Guideline
13. Privacy Notice Guideline
14. Records of Processing Activities Guideline
15. Special Nature Processing Guideline

Templates

1. Data Privacy Impact Assessment (DPIA) Template
2. Records of Processing Activities Template

Forms

1. Personal Data Breach Form
2. Special Nature Processing Permission Request

Checklist

1. Data Protection Self-Assessment

Advisory Notes

1. Building a Comprehensive Data Privacy Program
2. Personal Data Lifecycle Management

The list is subject to updates: (https://ncsa.gov.qa/en/pages/guidance-hub-for-regulated-entities

Tools

1. Vendor Privacy Management Tool
2. Organisation Level Privacy Compliance Assessment Tool
3. Privacy by Design Assessment Tool
4. Cloud Privacy Assessment Tool

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?”

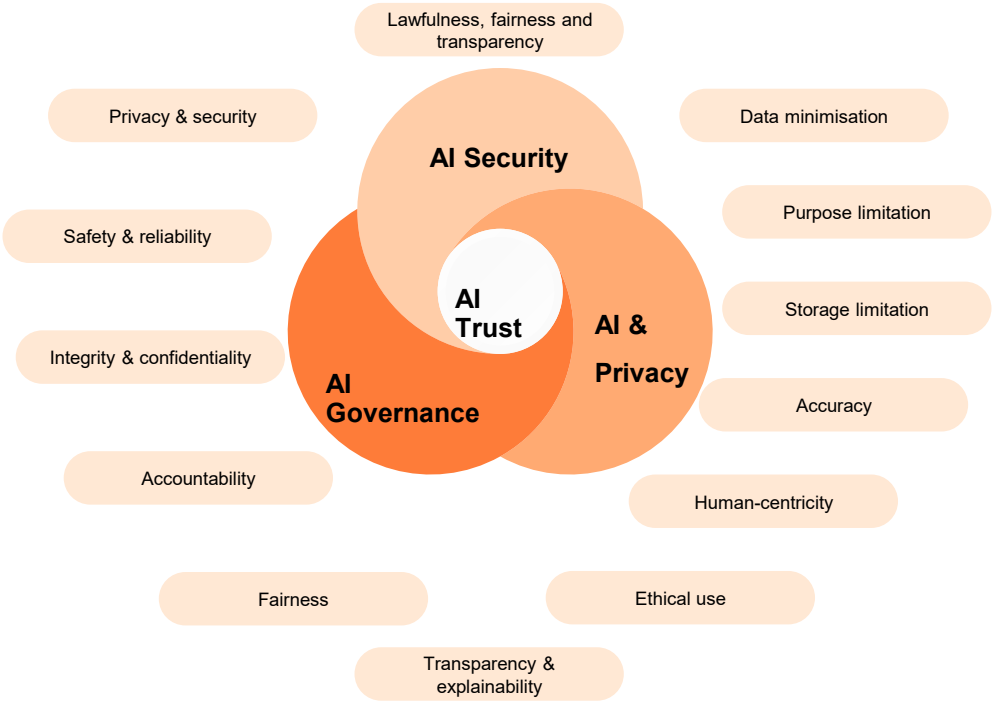
Where AI and Privacy intersect

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.



Example 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: 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.

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.

What is personal data?

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

Examples of personal data

- Name and surname
- ID card number
- Online identifiers (e.g. usernames, IP addresses)
- CCTV footage

Examples of non-personal data

- An organisation's corporate registration number
- 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 with special nature, as it could cause harm to the individual if leaked or misused.

While each data privacy law may have its own nuances, personal data is classified as ‘personal data with special nature’ if it relates to:

- **Children**
- **Ethnic origin**
- **Physical or psychological information**
- **Marital relations**
- **Religious creeds**
- **Criminal offenses**
- **Health**

Examples of personal data with special nature

- **Childrens' data**
- **Marital status**
- **Health records**
- **Religion**

It’s important to differentiate between personal data and personal data with special nature because the processing of personal data with special nature usually requires additional safeguards to be in place.

Organisations must request permission to process personal data with special nature and the NCSA has provided a form on its website: Special Nature Processing Permission Request form.

Individuals' rights

One of the aims of data privacy laws is to empower individuals and give them control over their personal data. Organisations must process all personal data within the bounds of transparency, honesty and respect for human dignity. If there is no permitted reason for the processing, the processing will be unlawful and in breach of the principle of honesty. The NCSA has published the Individuals' Rights Guideline to assist organisations.

- **Right to withdraw consent**
- **Right to protection and lawful processing**
- **Right to access their personal data**
- **Right to be notified of processing**
- **Rights to object to processing in certain circumstances**
- **Right to be notified of inaccurate disclosure**
- **Right to request correction**
- **Right to erasure***

In addition to the PDPPL, the NCSA have provided guidelines regarding individuals' rights that can be accessed on their website.

*Please note, not all data subject rights are 'absolute'. The 'right to erasure' is often misunderstood. The main reason for this is because many assume that it is an 'absolute right' whereas in actual fact there are only certain circumstances that people can request for their data to be deleted.

When can you process personal data?

The first principle of data privacy requires that all personal data be processed with transparency, honesty and respect for human dignity. To do so, organisations must have at least one of the following valid lawful bases for processing:

Consent

of the individual to the processing of their personal data.

Legitimate interests

of the organisation or the third parties engaged.

Contractual necessity

applies where processing is needed in order to enter into or perform a contract.

Legal obligation

for which the organisation is obliged to process personal data for.

Vital interest

of individuals, where processing is necessary to protect their lives.

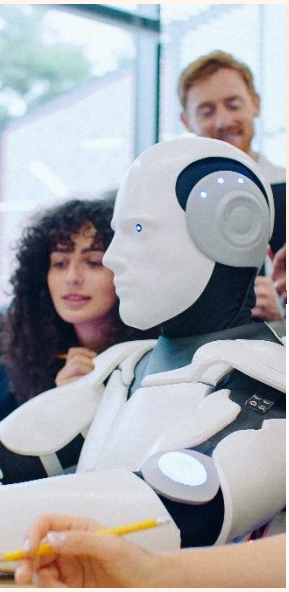
Public interest

specific to organisations exercising official authority or carrying out tasks in the public interest.

As different types of data require different levels of protection, data privacy laws specify different conditions for processing personal data with special nature and exemptions to the above lawful basis as outlined in the PDPPL:

- Personal data with special nature can usually only be processed with the individual's explicit consent, unless the data is for a task related to the public interest as per the law, implementing a legal obligation or an order by a competent court, vital interests achieving purposes of scientific research which is for public interest, or for information for an investigation into a criminal offense, upon an official request of investigative bodies.

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



Data privacy laws draw a clear distinction between data ‘controllers’ and data ‘processors’ to recognise that not all organisations involved with the processing of personal data have the same responsibilities.

Data controller: Controllers ‘determine the purpose of the processing’. This means that they make decisions about what information is captured and why.

Data processor: Processors process personal data on behalf of a controller and in line with the given instructions. If a processor sub-contracts some or all of the processing to another organisation, the latter is referred to as a sub-processor.

A simple way to think about this is as follows. A retailer creates an e-commerce website and decides what information 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.

Data controller or a data processor?

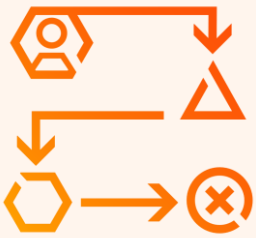
It is important to note that an organisation is not by its nature either a controller or a processor. It may be acting as a data controller for some personal data and processing activities, and as a processor for others.

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

02

Ten steps to an effective data

Privacy programme



Ten steps to an effective data privacy programme

01 **Appoint a Data Protection Officer, where applicable**

02 **Maintain a personal data register/ Records of Processing Activities (RoPA)**

03 **Ensure transparency and seek consent**

04 **Manage individuals' rights requests**

05 **Identify and enforce security mechanisms**

06 **Embed data privacy into your systems, processes and services**

07 **Handle personal data breaches**

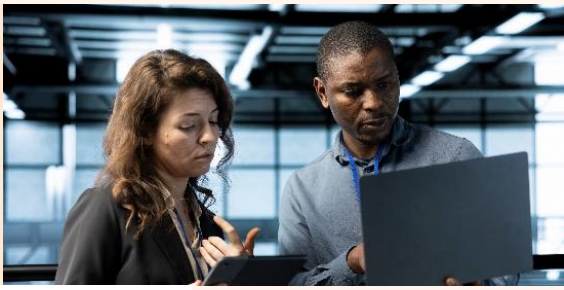
08 **Manage third parties**

09 **Control risks regarding cross-border data transfers**

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

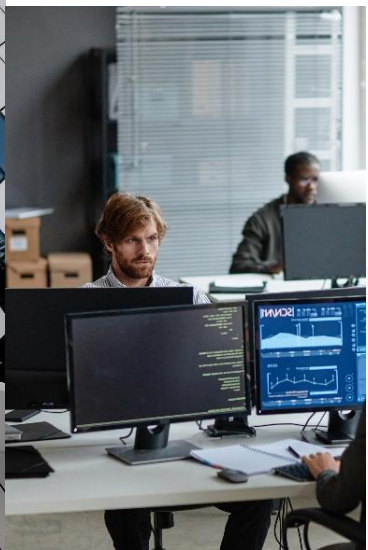
1 Appoint a Data Protection Officer

Many data privacy laws introduce the concept of a 'Data Protection Officer' (DPO), a leadership role for overseeing the organisation's data protection programme and ensuring compliance with the applicable laws. Under the PDPPL, at this time, this is not a mandatory requirement, under the PDPPL but it is encouraged.



What's the role of a DPO?

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



Who could act as a DPO?

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

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

2 Maintain a records of processing activities (RoPA)

In order to protect personal data, you need to know what data you collect, how you use it and where you store it. The first step in achieving this is identifying all processing activities in your organisation involving personal data and documenting how and why the data is used in what is called a personal data register, or Records of Processing Activities (RoPA). The NCSA has issued the Records of Processing Activities Guideline and template to support organisations.

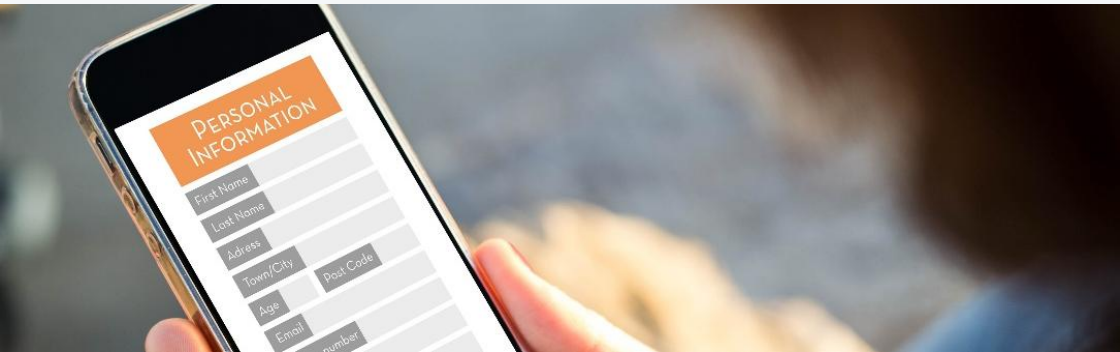
How can I identify personal data being processed?

Maintaining a RoPA is one of the key requirements of most data privacy regulations worldwide. 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?

Most data privacy laws require you to identify and document the following for every processing activity within your organisation, for example:

- Name and contact details of your DPO and any other third party (if applicable).
- The lawful purpose of processing the data.
- The different categories of personal data involved.
- The systems and locations where the personal data is processed.
- Where the data is transferred to and the list of recipients.
- The retention period and enforced technical and security measures (refer to page 24 for more details).



3 Ensure transparency and seek consent

Transparency is a central principle in data privacy laws. When collecting individuals' personal data you must provide them with clear information explaining why, what and how you're intending to process it.

What information should be provided to individuals?

The following should be included in the privacy information shared with individuals:

- Contact details of your organisation and DPO.
- Lawful purpose for processing, including details on legitimate interests if applicable.
- Recipients of personal data and details of cross-border transfers.
- Retention period of personal data and existence of automated decision-making.
- Details on individuals' rights, process for withdrawing consent and how to lodge complaints.

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?

Consent is a freely given, specific, informed and unambiguous agreement, provided by individuals through a statement or a clear affirmative action, to the processing of their personal data.
Consent means giving people control and choice over how their personal data is processed. It constitutes one of the legal grounds for lawfully processing personal data, however, there are conditions that need to be met to ensure its valid.

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)?

How can I be prepared?

To meet the defined timeline, your organisation has to implement robust procedures to authenticate the requester, assess the request and formulate an adequate response. The NCSA has published the Individuals' Rights Guideline to assist organisations.

What information should I provide?

- What personal data is being processed.
- The purposes for processing the data.
- Who within the organisation has the personal data and who it will be disclosed to.
- Whether or not the individual's personal data is used in any automated decision making (such as credit worthiness) and how that automated decision-making works.
- How long the data will be retained for, or at least the criteria used to determine this period.

What are the steps to responding to a data subject request?

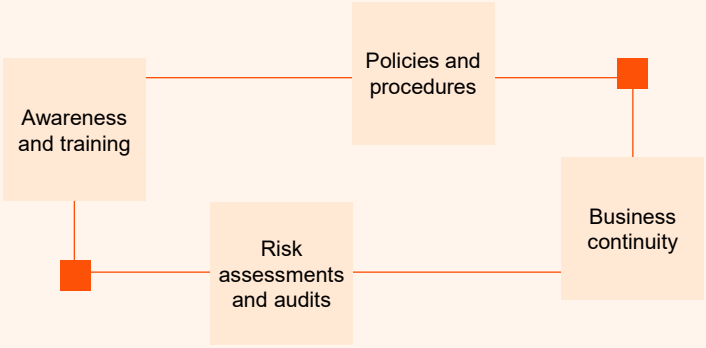
1. Receive the data subject request and forward it to the concerned department.
2. Determine if the request is self-raised or on behalf of others, then verify the identity of the individual.
3. Assess the request and confirm if an extension or charges are to be applied, as per the data privacy laws you are subject to. If so, respond to the individual providing explanation for time extension and/or admin charges.
4. Determine where the personal data of the individual is stored, be it in systems or physical documents.
5. Perform the appropriate action according to the type of data subject request (i.e. copy data, delete data, restrict processing, etc.).
6. Provide appropriate details to the DPO for delivery and response to the data subject.
7. Send and document the appropriate response to the individual.

5 Enforce security mechanisms

The PDPPL requires organisations to take appropriate administrative, technical and financial measures to protect personal data. This usually 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. The NCSA has published the Personal Data Management Systems (PDMS) Checklist to assist organisations.

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

Administrative and financial measures are defined as organisational controls, such as policies, procedures, training, budgeting, and resourcing, put in place to ensure compliance with the law and protect personal data.



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

Data privacy laws have introduced detailed requirements on privacy by design and default. The NCSA has published the Data Privacy by Design and by Default and a tool assessment to assist organisations. A first step to translate these broad concepts into functional requirements is to define their key principles as follows:

Privacy and data protection are embedded into the design of a new process or application

01

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

02

Safeguards are established and enabled (example: enforcing encryption and data minimization mechanisms on personal data)

03

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. As data privacy regulations introduce strict reporting timelines, it is crucial for every organisation to be well prepared in the event of a data breach. The NCSA has published the Personal Data Breach Notifications Guideline and Data Breach Form to assist organisations.

How do I respond to a data breach?

Within a limited time (depending on the data protection law in question) after a data breach
has been discovered, you must:

- Assess the nature of the breach and confirm if personal data is involved.
- Identify what personal data has been impacted and how.
- Assess the impact of the breach to determine if it poses high risk to the rights and freedoms of individuals.
- Determine if you need to notify the Authority and the individuals concerned.
- Carry out a thorough investigation to identify the source of the breach.

What is data privacy by design?

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

- Nature of breach (who accessed what and when, what caused the breach, how was the data used, who are the affected individuals)
- Description of the estimated impact and possible effects.
- Contact details of your data protection supervisor.
- Procedures taken by your organisation 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

Data privacy laws deepen obligations around third-party risk management. If you engage a third party to process personal data, you may be held responsible if your service provider violates applicable data privacy laws while providing the service to you. The NCSA has provided a Vendor Privacy Management Tool to assist organisations.

When entering into a contractual agreement with your service provider, ensure there are clauses that require them to take sufficient measures to ensure compliance with the requirements of 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 subject-matter and duration of processing
- The nature and purpose of processing
- The type of personal data and categories of Individuals
- The minimum terms or clauses required of the processor
- The obligations and rights of the controller

What is data privacy by design?

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.

9 Control risks regarding cross-border data transfers

With a significant number of organisations' operations spanning several countries and territories, data transfers are an integral part of today's global economy. Many data privacy laws contain a 'whitelist' of countries to whom personal data may freely be transferred because they provide adequate levels of personal data protection. For non-whitelisted countries or 'third countries' as they are also known, data privacy laws usually require safeguards to be in place whenever data is transferred to such places. Often this means using a recognised data transfer mechanism.

What is considered a third country data transfer?

A third country data transfer is the transfer of personal data to a country or jurisdiction where the data privacy law of the sender's country does not apply, and which has not been assessed as providing an adequate level of data protection when compared with the sender's home country. You are making a cross-border data transfer if:

- The personal data that you intend to transfer is in scope of one or more data privacy laws
- The personal data is transferred to a third country
- The receiver is a separate organisation or individual. This also covers transfers to another company within the same corporate group

When can I transfer personal data?

Transferring personal data cross-border is permissible while ensuring that any transfer outside Qatar complies with PDPPL and does not cause serious damage to personal data or privacy. This should be backed by a documented Data Protection Impact Assessment and PDPPL-compliant contractual safeguards.

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 Qatar PDPPL. 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 NCSA has published the following to assist organisations Data Checklist a Protection Self-Assessment and Advisory Note on Building a Comprehensive Data Privacy Program and Personal Data Lifecycle Management.

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

Qatar PDPPL 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

03

Nine 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 applicable data 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

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

Ongoing operations and monitoring

What is provided
- Defined ongoing monitoring programme
- Tracking and retesting of non-compliance
- Protocols for changes to policies and procedures

Gap assessment and roadmap

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

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

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.

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.