

Data Privacy Handbook

A starter guide to data
privacy compliance



Contents

04

A quick introduction to data privacy



06

About this handbook



07

Why is data privacy important?



08

Key concepts



09

Key principles of data privacy



10

What is personal data?



11

What is sensitive personal data?



12

Controllers vs. processors



14

Individuals' rights



15

When can personal data be processed?



16

Ten steps to an effective data privacy programme



A quick introduction to data privacy

There are many definitions for 'data privacy'. The simplest way to think about it is that people (customers, employees, anybody!) need to know what personal data organisations are collecting about them and how they are using it. Of course, this is a simplistic way to look at the topic but it is useful to set the scene.

Data privacy is far more than just the security and protection of personal data. It all boils down to how organisations are using that personal data. Organisations need to process personal data in an ethical and legal manner. That could mean not bombarding customers with unwanted SMS marketing messages but it could also mean simply not sharing personal information with third parties without the customer's consent. It doesn't mean that

marketing is now forbidden under data privacy laws but it does mean that organisations need to be transparent about what personal data they are capturing and how it's going to be used. Many organisations recognise the significant risks of cyber attacks and data breaches but fail to understand what else is required to safeguard what is referred to as the "rights and freedoms of individuals".





In the past year there were a series of high-profile data breaches followed by mega-fines from regulators. This has increased awareness about the importance of data privacy and protection. The European Union (EU) also introduced the “General Data Protection Regulation” (GDPR), which set stricter standards for data privacy and protection and further increased awareness around the importance of data protection compliance.

In the Middle East, some GCC States have already adopted their own privacy laws and other states have signalled their intent to release similar legislation in the near future. Many of the recent data privacy laws, including local Middle East data protection laws, have striking similarities with the GDPR. This is not surprising because the GDPR radically overhauled data privacy practices and is now considered the gold standard in data privacy, worldwide.



About this handbook



The data privacy landscape is complex and it continues to evolve. It presents many challenges to organisations by creating uncertainty on many levels about whether, how, and when to process personal data. The complex implementation of the GDPR and the continuing efforts worldwide to draft local data privacy regulations are having a serious impact on organisations' abilities to update and align their business practices to the ever-changing regulatory requirements.

We've put together this Data Privacy Handbook to try to simplify the requirements and help you kick-start your data privacy compliance journey. The toolkit contains useful information and resources to help you assess your current business processes against data privacy best practices and take the necessary steps to improve them.

This toolkit reflects best practices aligned to the requirements of the GDPR, requirements and practices specific to the Middle East region and PwC's own proprietary frameworks. The toolkit is suitable for all organisations processing personal data and looking for a practical approach to build their data privacy programmes, be it to comply with privacy regulations or to gain competitive advantage.

Why is data privacy important?

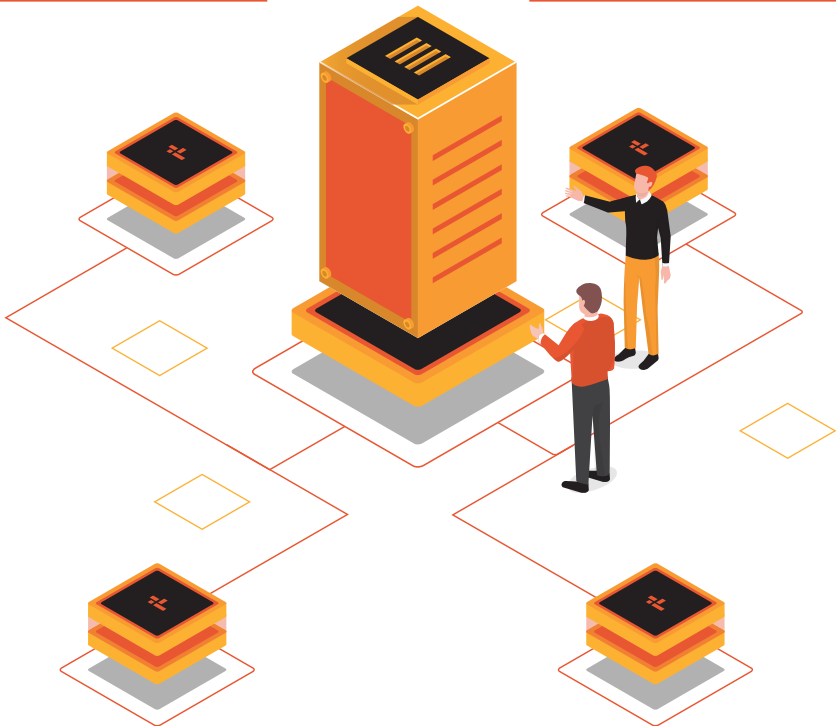
Companies that fail to protect personal data and comply with data privacy regulations aren't just risking financial penalties. They also risk operational inefficiencies, intervention by regulators and most importantly permanent loss of consumer trust.

Regulatory

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

Reputational

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



Financial and criminal

Fines and, in some countries potential prison sentences, could be enforced depending on the violation. You may also experience loss of revenue and high litigation and remediation costs.

Operational

Most data privacy laws give people more rights over their data, such as the right to access their data or the right for it to be deleted. This can be a significant operational burden if it is not implemented effectively.

Key concepts

Data privacy laws introduce a number of new terms and concepts which are important for you to familiarise yourself with, before continuing.

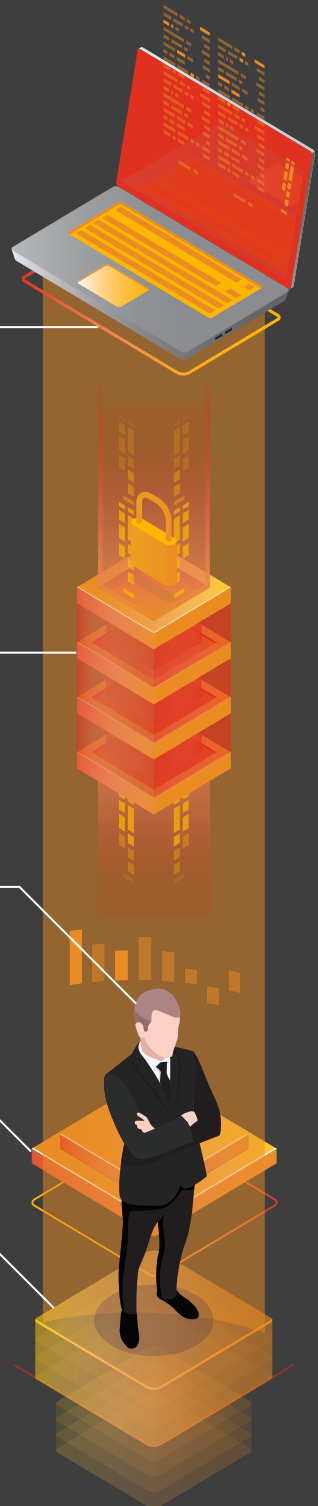
'Data processing' or 'Processing' means any automated or manual operation(s) carried out on personal data. In essence, this covers almost any relevant action word that could possibly be performed on information including collecting, recording, organising, classifying, storing, modifying, amending, retrieving, using or revealing such data by broadcasting, publishing, transmitting, making available to others, integrating, blocking, deleting or destroying.

'Data protection authority' or 'Authority' is the national body established to be responsible for upholding the rights of individuals to the protection of their personal data through the enforcement and monitoring of compliance with the local data privacy laws.

A **'Data Subject' or 'Individual'** is defined as the person to whom the personal data relates.

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

'Sensitive personal data' is a subset of personal data and is defined as information that directly or indirectly reveals a person's race, ethnicity, political or philosophical views, religious beliefs, union affiliation, criminal record or any data related to their health or sexual life. Refer to page 5 for further details.



Key principles of data privacy

Most data protection laws are built on a set of key principles, which establish the foundation for everything related to data privacy and the protection of personal data.

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

The principles are:

Lawfulness, fairness and transparency

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

Purpose limitation

You should only process personal data for a specified and lawful purpose.

Data minimisation

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

Accuracy

You should ensure personal data is kept up to date, and that necessary measures are in place for correcting and updating inaccurate data.

Storage limitation

You must not keep personal data for longer than you need it.

Integrity and confidentiality

You must implement adequate security controls to ensure that personal data is protected against loss, destruction or damage.

Accountability

You must have appropriate measures and records in place to be able to demonstrate your compliance.



What is personal data?

Personal data is any information that can identify 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.

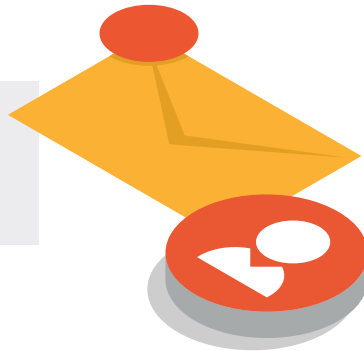


Examples of personal data

- 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, licence plate number.

What is sensitive personal data?

Some personal data is considered sensitive, as it could cause harm to the individual if leaked or misused. While each data privacy law may have its own nuances, personal data is classified as 'sensitive' if it relates to:

- » Racial or ethnic origin
- » Political or religious beliefs
- » Trade union membership
- » Physical or mental health
- » Sex life or sexual orientation
- » Criminal offences and court proceedings



Examples of sensitive personal data

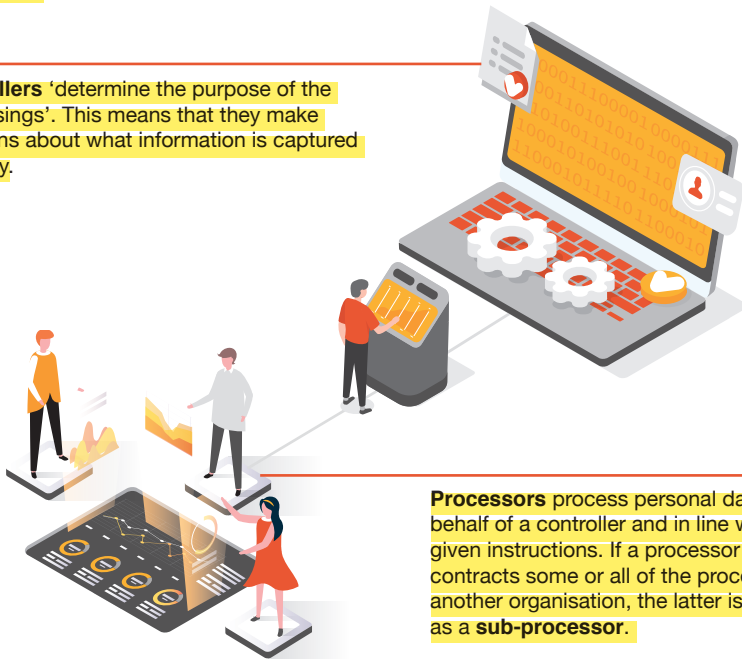


It's important to differentiate between personal data and sensitive personal data because the processing of sensitive personal data usually requires additional safeguards to be in place.

Controllers vs. processors

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.

Controllers 'determine the purpose of the processings'. This means that they make decisions about what information is captured and why.



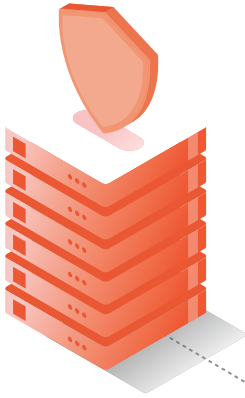
Processors process personal data on behalf of a controller and in line with the given instructions. If a processor sub-contracts some or all of the processing to another organisation, the latter is referred to as a **sub-processor**.

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.

Am I a controller or a 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 controller for some personal data and processing activities, and as a processor for others.

What does it mean if I am a..



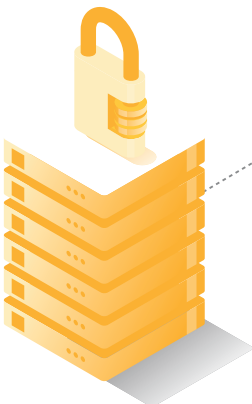
Data controller

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

Processor

You have less autonomy over the data you're processing, but you may still have direct legal obligations. If you engage a sub-processor, you may be liable to the controller for the sub-processor's compliance.

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



Sub-processor

As a sub-processor, you may be liable for any damage caused by your processing in case you have not complied with your legal obligations and if you failed to follow the controller's instructions. Your responsibilities towards the processor are similar to the processor's responsibilities towards the controller.

Individuals' rights

One of the aims of data privacy laws is to empower individuals and give them control over their personal data. Therefore, most data privacy laws introduce what are usually referred to as 'data subject rights' concerning the protection of individuals' personal data. It's important to note that not all of these rights are 'absolute', meaning some only apply in specific circumstances:

Right to limit personal data processing

Individuals have the right to request the restriction of the processing of their personal data.

Right to access personal data

Individuals have the right to access and request copies of their personal data.

Rights related to automated decision making and profiling

Individuals can object to decisions made about them based solely on automated and mechanical processing.

Right to erasure*

Individuals can have their personal data deleted without undue delay.

Right to correct personal data

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

Right to transfer personal data

Individuals have the ability to receive data in an organised, commonly used machine-readable form.

Right to objection

Individuals can object to the processing of their personal data by an organisation.



*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 personal data be processed?

The first principle of data privacy requires that all personal data be processed lawfully and fairly. 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 interest: of the organisation or the third parties engaged.

Contractual necessity: 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 sensitive and criminal data:

- **Sensitive data** can usually only be processed with the individual's explicit consent, unless the data is required for filing legal proceeding or claims, or if there is any legal, public interest or regulatory requirement.
- Personal data relating to **convictions and criminal offences** can usually only be processed as long as it is carried out under the control of a certain government authority or in accordance with local laws.

Top tips

- You must determine your lawful basis before you begin processing, and you should document it.
- Get it right the first time - you should not swap between bases at a later date.
- If your purposes change, you need to reassess the new purpose and determine a valid lawful basis.



Ten steps to an effective data privacy programme



1

Appoint a Data Protection Officer

18

2

Maintain a personal data register

19



3



Notify purpose and seek consent

20

4

Respond when individuals ask about their personal data

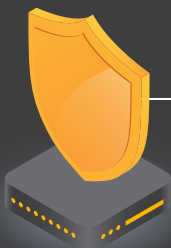
21



5

Enforce security mechanisms

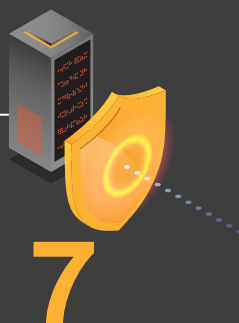
22



6

Embed data privacy into your systems, processes and services

24



7

Notify data breaches

26



8

Manage third parties

27



9

Protect personal data when transferring overseas

28



10

Communicate your data protection policies, practices and processes

30



17

1

Appoint a Data Protection Officer

Many data privacy laws introduce the concept of a 'Data Protection Officer' (DPO), a new leadership role for overseeing the organisation's data protection programme and ensuring compliance with the applicable laws.

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.

What's the role of a DPO?

The DPO assists you in monitoring internal compliance with the applicable 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.



2

Maintain a personal data register

In order to protect personal data you need to know what data you collect, how you use it and where you store it. The first step in achieving this is identifying all processing activities in your organisation involving personal data, and documenting how and why the data is used in what is called a 'personal data register'.

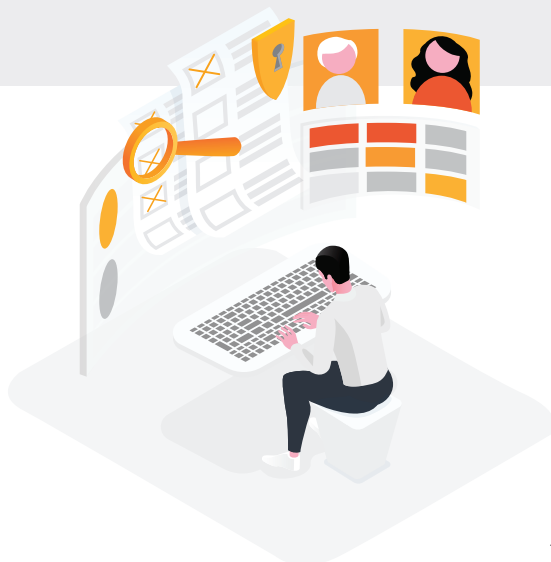
How can I identify personal data being processed?

Maintaining a personal data register 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:

- Name and contact details of your DPO and any other third party (if applicable).
- The lawful basis and 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 Notify purpose 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 I provide?

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

- Contact details of your organisation and DPO.
- Purpose and lawful basis 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 it's valid.

How can I obtain consent?

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



4

Respond when individuals ask about their personal data

What are data subject requests?

Data privacy laws introduce new rights for individuals that are designed to give them more control over how their data is used. Individuals are entitled to raise requests to exercise their data subject rights and organisations must respond within a specified period, as per the data privacy laws you are subject to.

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.



What information should I provide in my response?

- What personal data is being processed. Refer to page 9 for further details.
- 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?

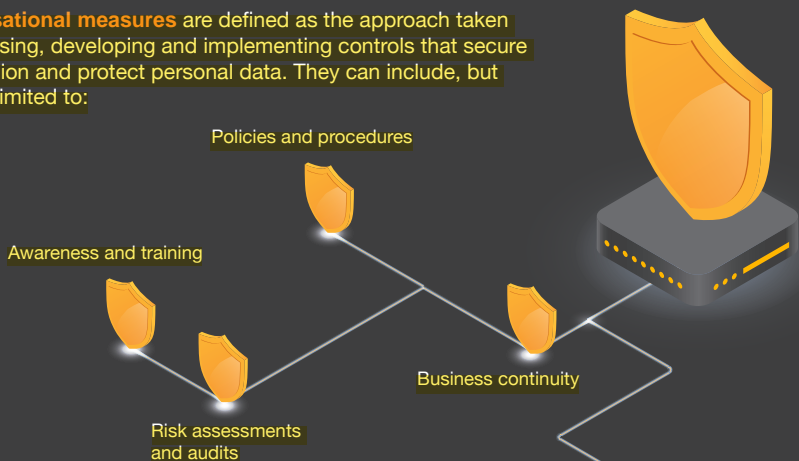
1. Receive the data subject request and forward it to the concerned department.
2. Determine if the request is self-raised or on behalf of others, then verify the identity of the individual.
3. Assess the request and confirm if an extension or charges are to be applied, as per the data privacy laws you 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

Most data protection laws require organisations to ensure that 'organisational and technical measures' are in place to protect personal data. This usually means that organisations need to take reasonable steps to protect personal data. What is 'reasonable' will usually come down to a business decision with the support of legal counsel, and will be based on the organisation's size and the amount and type of personal data being processed.

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

Organisational measures are defined as the approach taken in assessing, developing and implementing controls that secure information and protect personal data. They can include, but are not limited to:



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

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



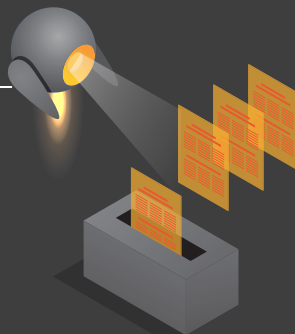
Which security measures should I implement?

Depending on the size of your organisation and the processing activities undertaken, there are a broad range of technical and organisational measures that can aid in securing and protecting personal data. We also suggest utilising established frameworks such as ISO27001 to assess and develop adequate measures.

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

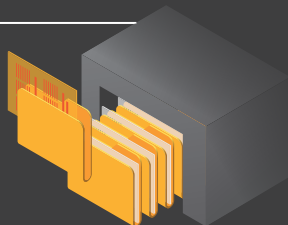
Step 1

Carry out an information security risk assessment by reviewing the personal data you hold, the way you use it, and the risks presented by the processing.



Step 2

Carry out a technical vulnerability assessments (e.g. a penetration test) on devices and systems posing high risk on your personal data processing.



Step 3

Assess and select the most adequate security measures to mitigate the identified risks.



Step 4

Ensure your employees are kept up to date on your information security programme and latest security best practices.



6

Embed data privacy into your systems, processes and services

Recent data privacy laws have introduced detailed requirements on privacy by design and default. A first step to translate these broad concepts into functional requirements is to define their key principles as follows:

1. Privacy and data protection are embedded into the design of a new process or application (example: creating a corporate culture where privacy and data protection are tone-at-top).

2. Accountability is communicated and supported (example: conducting internal audit reviews over data privacy programme and practices).

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

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

While these principles help to inform the organisation's overall approach, successful privacy by design and default is facilitated by governance and oversight, implemented by a supportive workforce, and informed by risk and compliance.

What is 'data privacy by default'?

Data privacy by default links to the fundamental data protection principles of data minimisation and purpose limitation.

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

- adopting default privacy settings on systems;
- being transparent with your customers and employees on your data processing activities and practices;
- processing data that is proportionate to the purpose; and
- providing information and options to individuals to exercise their rights.



What is 'data privacy by design'?

Organisations committed to providing an environment that safeguards personal data must embed data privacy 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
- Transferring data to a new third party
- New or changing business process
- New product offering
- New use of existing data to improve a product or service



Privacy by design is mainly comprised of two distinct elements:

1. Data Privacy Impact Assessment (DPIA): a tool used to identify privacy risks of processing activities, assessing their impact and designing controls to mitigate the identified risks and implement privacy requirements.
2. Personal Data Change Management: a process outlining the five general phases to be integrated within a project's implementation lifecycle, from inception to completion.

Privacy by design requires you to:

- put in place appropriate technical and organisational measures designed to implement the data privacy principles; and
- embed controls into your processing activities so that you meet the legal requirements and protect individuals' rights.

7

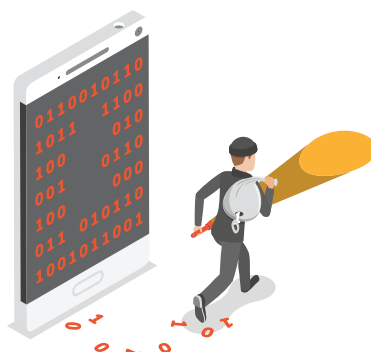
Notify data breaches

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.

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.



Notifying the Authority

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 to beat the clock

- 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 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 add new requirements and 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.

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?

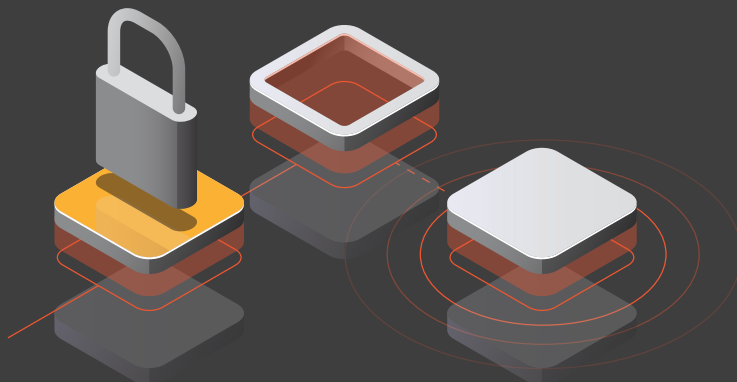
Contractual agreements with third parties should at a minimum include the following details:

- The subject-matter and duration of processing
- The nature and purpose of processing
- The type of personal data and categories of data subjects
- The minimum terms or clauses required of the processor
- The obligations and rights of the controller

Enhancing your third party risk management programme

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

- Conduct a due diligence assessment to ensure that the third party has adequate controls in place to protect personal data.
- Update your existing contracts and draft new contracts clearly defining the roles, responsibilities and liabilities of both parties.
- Continue to improve ongoing monitoring through risk assessments and audits to ensure that third parties are maintaining adequate controls to protect personal data.



9

Protect personal data when transferring overseas

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 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 overseas can pose higher risks to the organisation. In certain circumstances, data privacy laws restrict transfers of personal data outside their jurisdictions unless certain safeguards are in place.

Which safeguards are considered appropriate for personal data transfers?

There are a number of mechanisms your organisation could adopt to protect personal data when transferring to third countries. Some safeguards recognised by the GDPR are:

Binding Corporate Rules (BCRs):

Legally binding and enforceable internal rules and policies for data transfers within multinational group companies that allow intragroup data transfers to countries that do not provide an adequate level of protection for personal data. BCRs usually need to be approved by an Authority.

Standard contractual clauses:

A set of standard clauses, provided by a relevant Authority, to be used in contracts.

Code of Conduct:

These resemble self-regulatory programmes to demonstrate to regulators and consumers that a company adheres to certain data privacy standards.

Certification:

Granted to the receiver, under a scheme approved by the Authority. The certification scheme must include appropriate safeguards to protect the rights of individuals whose personal data is transferred, and which can be directly enforced.

What if the cross-border transfer is not covered by appropriate safeguards?

If the transfer is not covered by appropriate safeguards, then you need to assess if one of the exceptions defined in the applicable data privacy laws applies. These exceptions are specific for each data privacy law and could include relying on the individual's explicit consent or entering in a contract with the individual.

10 Communicate your data protection policies, practices and processes

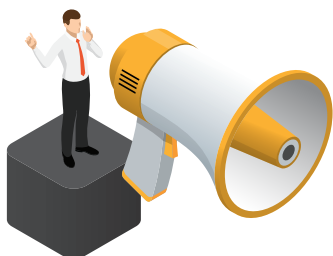
Complying with data privacy laws is not something that can be left to the legal and compliance departments alone. Compliance with data privacy laws requires that everybody in the organisation understands their responsibilities to protect personal data. It is very important to communicate your data privacy policies and practices to your customers and employees to ensure they are familiar with how you process and protect personal data.

Customers

- Make the business contact information of your DPO easily accessible so that your customers know who to contact for inquiries or complaints.
- Readily provide information about your data protection policies, practices and complaints process upon request.
- Update your privacy notice to make sure your customers understand what personal data you process, and how you do it, to enable them to make informed decisions about it. The privacy notice should be:
 - Concise and transparent
 - Written in clear and plain language
 - Delivered in a timely manner
 - Made publicly available and easy to access






Employees

- Communicate your data protection policies and practices to your employees to make sure they are familiar with their roles and responsibilities in processing personal data.
- Develop a culture of privacy awareness within your organisation by aligning the importance of data privacy to your values and implementing practical approaches to convert it to repeated practices.
- Use posters, email and other communication tools to raise awareness of the importance of personal data protection among your staff.
- Send key employees who handle personal data to attend regular data privacy training to ensure they are kept up to date on your internal processes and latest developments in the privacy space.



How PwC can help

As experts in data privacy, we are well positioned to support you with your organisation's journey to data privacy compliance. We have developed a five step approach to transforming privacy programmes, with tools and accelerators to assist the process.

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

Get in touch

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

**Phil Mennie**

Partner, Middle East Data Privacy
Leader
phil.mennie@pwc.com
[linkedin.com/in/philmennie](https://www.linkedin.com/in/philmennie)

**Nabil Diab**

Partner, Egypt
nabil.diab@pwc.com
<https://www.linkedin.com/in/nabil-diab-pwc>

**Richard Chudzynski**

PwC Legal
richard.chudzynski@pwc.com
[linkedin.com/in/richardchudzynski](https://www.linkedin.com/in/richardchudzynski)

**Tamer Amin**

Director, Egypt
tamer.amin@pwc.com

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 158 countries with over 250,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

Established in the Middle East for 40 years, PwC has 22 offices across 12 countries in the region with around 5,200 people. (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.