SDAIA
الهيئة السعودية للبيانات والذكاء الاصطناعي
Saudi Data & AI Authority

Guide to

the Saudi Personal Data Protection Law

Version1.0
December 2023

Executive Summary

What is data protection?

Data protection is a set of principles, practices and measures aimed at safeguarding individuals' personal data and ensuring compliance with data protection laws and regulations. A well-designed data protection compliance program is fundamental to enable you to be compliant with the principles and requirements of the PDPL.

While data protection is not explicitly mentioned in the Kingdom's Vision 2030, it is closely interlinked with the Vision's goals of digital transformation, digital economy, transparency, innovation, and building a data-driven economy. As such, data protection is fundamental to achieving these objectives.

This guide covers three sections that will introduce you to the various data protection requirements of the PDPL. This guide will be your on-the-job reference in your data protection compliance journey. Each of the key requirements of the PDPL is explained through examples, including some best practice requirements. While the examples are contextualized for a certain sector, please note that you must comply with the PDPL, regardless of the sector in which you operate.

Section A: Why is data protection important to Vision 2030?

Vision 2030 is closely linked to digital transformation and the development of a knowledge-based economy. In this context, data protection is very important for the growth and prosperity of the Kingdom. Here is how data protection is connected to Vision 2030.

• Develop the Digital Economy:

Vision 2030 aims to foster the growth of a digital economy by promoting innovation and technological advancements. As digital technologies become more widespread, the need for data protection becomes crucial to ensure the privacy, security and trust of individuals and businesses regarding such technologies.

• Enhance transparency across government roles:

Vision 2030 emphasizes the development of efficient and transparent e-government services. As government entities collect and process large amounts of personal data, it becomes essential to implement strong measures to protect such personal data.

• Nurture and support the innovation and entrepreneurship culture:

Robust data protection measures foster trust and confidence for startups and organizations, enabling secure handling of customer personal data and protecting intellectual property rights. Data protection builds trust and consumer confidence.

• Data-driven Decision Making:

Vision 2030 assumes extensive use of data analytics and insights for the benefit of policy-making, economic planning and business strategies. Effective data protection is necessary to ensure the integrity, accuracy and ethical use of data.

In the Kingdom specifically, the processing of personal data is regulated by the Saudi Data and AI Authority ("SDAIA").

In this guide, "processing" of personal data means any kind of use of personal data.

Section B: Starting your data protection compliance journey

A. Understanding the PDPL and the Implementing Regulations

Before starting your data protection compliance program, you must have a detailed understanding of the PDPL's key principles, legal requirements and obligations. This also includes understanding the legal bases for processing personal data, the rights of individuals and your obligations regarding data transfers outside the Kingdom.

B. Understanding the Personal Data that you hold

By understanding what personal data is[1] and what personal data you use, you can identify the types of personal data you process, determine a legal basis for processing and implement the appropriate safeguards for such personal data. The first step is to perform data discovery. Based on the data discovery, you will be able to prepare the Record of Processing Activities ("RoPA"), as required by the PDPL.

01 Performing Data Discovery

For effective data protection, it is crucial to perform data discovery within your organization to understand what personal data you use. You can start by identifying all the data you collect, store and process. This includes structured and unstructured data, both in electronic and physical formats, confidential and non-confidential data. You must assess where the personal data is stored, who has access to it and how it is used. To improve the quality of the data discovery, you should conduct interviews with relevant stakeholders[2] within your organization, review data flows and (where possible) use automated tools for data discovery.

02 Determining a Legal Basis of Processing

Choosing a suitable legal basis for data processing is one of the key requirements of complying with the PDPL. Depending on the purpose of processing, you must select a suitable legal basis from those specified in the PDPL. Such legal bases include consent, legitimate interest, contract performance, legal obligation, etc.

03 Establishing the Records of Processing Activities (RoPA)

As part of your data protection compliance program, you are required to establish and maintain comprehensive records of processing activities. Once you complete your data discovery, you must document information on the purposes of processing, data categories, recipients, data transfers, retention periods and data security measures implemented. You must ensure that these records are regularly updated so that they reflect any changes in your data processing activities.

04 Developing and Publishing Privacy Notices

One of the key requirements of the PDPL is to develop and publish privacy notices so that you meet your transparency requirements. Privacy notices play a crucial role in providing transparency and promoting trust between you and individuals whose personal data you process. These notices inform individuals of what personal data will be collected, as well as how their personal data will be collected, used and protected on an ongoing basis. In essence, a privacy notice empowers individuals to make informed decisions about their personal data.

[1] Personal data is any information that can directly or indirectly identify an individual.

[2] The relevant stakeholders are those employees of your organization who are extensively involved in the use of personal data or who understands the legal requirements to its processing. Usually these are the heads of such departments, as IT, HR, Legal, Compliance, etc.

C. Establishing Accountability and Governance

For a successful data protection compliance program, it is very important to establish accountability within your organization. This includes, for example, appointing a Data Protection Officer, where applicable, developing a data protection governance structure, establishing policies and procedures to demonstrate compliance with the PDPL, etc.

01 Assessing the Need for and Appointing a Data Protection Officer (DPO)

Where applicable, you must designate a DPO to oversee your data protection compliance program. The DPO must have the necessary expertise in data protection and must operate independently. The DPO's responsibilities include, amongst other things, monitoring ongoing compliance with the PDPL, providing advice on matters related to data protection and acting as a point of contact for data subjects and the competent authority.

In this guide, "data subjects" means all individuals whose personal data you process.

02 Establishing a Data Protection Governance Structure

When setting up a robust data protection compliance program, it is essential to establish a strong governance structure. You can start by creating a framework that ensures accountability, transparency and effective decision-making regarding data protection practices within your organization. You must ensure that data protection roles, responsibilities and reporting lines are clearly defined in your internal documents. You must appoint individuals or committees responsible for overseeing compliance.

03 Developing Policies, Procedures and Conducting Training

You must also develop and implement comprehensive internal data protection policies and procedures. These must include clear guidelines on how personal data must be processed, stored and shared within your organization. In addition, you must also develop procedures for handling personal data breaches and other complaints that may be received. You must also conduct regular training and awareness programs to ensure your employees understand their roles and responsibilities in protecting personal data

04 Implementing Processes for Individual Rights Requests

Individual rights are a fundamental aspect of the PDPL. These rights empower and grant individuals control over their personal data through a number of means, for example, the right to access, rectify, and erase their personal data. You must respond promptly and transparently to individual rights requests. With the use of such rights, individuals have the ability to manage their personal data in accordance with the PDPL.

D. Conducting Impact Assessments

Where applicable, you must perform an impact assessment for certain processing activities. This is an assessment that helps identify and mitigate data protection risks associated with the processing of personal data. At the minimum, impact assessments must be carried out in cases required by the PDPL. They help you to ensure that data protection risks are minimized to an acceptable level with a documented mitigation plan.

Please note that in the context of Art. 12, the term "privacy policy" means "privacy notice".

E. Privacy by Design and Default

Privacy by Design and Default, although not strictly required under the PDPL, is strongly encouraged to be embedded into all stages of your personal data processing lifecycle. It is a requirement to implement technical and organizational measures that ensure data protection in all your systems, products and services. This includes implementing appropriate security measures, limiting data collection to the minimum extent possible, limiting retention of personal data to specific timelines and obtaining consent from your data subjects, where necessary.

F. Implementing Personal Data Breach Handling Procedure

You must establish procedures for detecting, reporting and managing personal data breaches. You must ensure notification of the data breach to the competent authority and affected data subjects, where required by the PDPL. Personal data breach response plans must be developed and tested regularly to ensure their effectiveness. In any case, where you experience a personal data breach, it should be thoroughly investigated to identify its causes and to prevent future breaches.

G. Implementing Technical and Organizational Measures

Implementing technical and organizational measures is a proactive measure to safeguard personal data. Technical measures include cybersecurity technologies and controls that help safeguard data against personal data breaches. Organizational measures involve the implementation of policies, procedures, and training to promote data protection awareness and accountability among employees and stakeholders within your organization. By combining technical and organizational measures, you can establish a comprehensive data protection framework that mitigates risks, promotes trust and ensures ongoing compliance with the PDPL.

H. Sharing Personal Data within the Kingdome

While personal data sharing within the Kingdom may seem straightforward, it still requires adherence to the PDPL's requirements to protect personal data and individuals' rights. You must ensure that appropriate technical and organizational measures (including legal safeguards) are in place to protect personal data during its sharing and processing.

I. Transferring Personal Data outside the Kingdom

Transferring personal data outside the Kingdom involves moving personal data from the Kingdom to another jurisdiction. This process has become increasingly common, driven by international business operations and data-sharing practices. However, transferring personal data across borders requires careful consideration of data protection laws and regulations in both the exporting and importing jurisdictions. You must take measures to ensure that personal data are always protected and individuals' rights are respected, as laws may vary significantly between jurisdictions.

J. Monitoring and Auditing Compliance

Regular monitoring and auditing are essential to staying compliant with the PDPL and your organization's policies. This includes conducting internal audits, reviewing personal data processing activities and verifying the effectiveness of data security measures. Results from monitoring and audits should be documented, and corrective actions should be taken promptly to address any identified gaps.

In essence, establishing and operationalizing a data protection compliance program is essential for you to achieve compliance with the PDPL. By following the initiatives outlined in this guide, you can establish good data protection practices, mitigate data protection risks and build a culture of data protection within your organization.

Section 01

Understanding the PDPL and the Implementing Regulations

Understanding the PDPL is essential for developing a comprehensive data protection compliance program. The PDPL outlines the rights and obligations related to any operation carried out on personal data by any means. By understanding the PDPL, you can have a clear understanding of the data protection requirements in the Kingdom. The Implementing Regulations provide details on how general rules of PDPL must be implemented.

A. PDPL Principles

Although the PDPL does not explicitly list data protection principles, such principles are embedded in the PDPL's provisions. Understanding these principles will help you understand many of the requirements of the PDPL.

▶ There are seven key data protection principles:

- **Lawfulness, fairness and transparency:**

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

- **Purpose limitation:**

You must only process personal data for a specific and lawful purpose.

- **Data minimization:**

You must only process the personal data that you truly require to achieve the purpose of processing.

- **Accuracy:**

You must ensure that 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 data security controls to protect personal data against loss, destruction or damage.

- **Accountability:**

You must have appropriate measures and records in place to demonstrate your compliance with data protection laws, regulations and principles.

B. What are the Rights of an Individual Under the PDPL?

One of the aims of the PDPL is to empower individuals and give them control over their personal data. As such, the PDPL sets out a list of the individual's rights. Please note that not all of these rights are absolute, and some of them only apply under specific conditions.

▶ Individuals have the following rights under the PDPL:

03 Right to be informed:

Individuals have the right to be informed about the lawful basis for the collection of their personal data, as well as of the purpose (aim) of such collection.

04 Right to access personal data:

Individuals have the right to access their personal data subject to meeting the requirements of the PDPL and its Implementing Regulations

05 Right to request provision of personal data:

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

06 Right to request correction:

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

07 Right to request destruction:

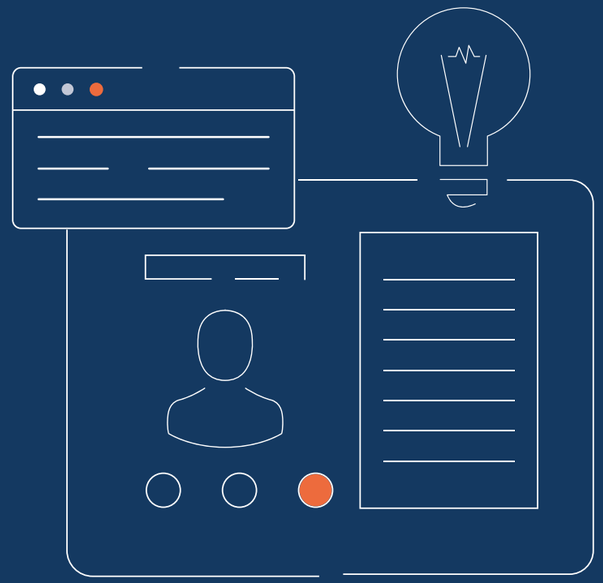
Individuals can request destruction (erasure) of their personal data.

08 Right to withdraw consent:

Individuals can, at any time, withdraw their consent to the processing of their personal data.

Section 02

Understanding the Personal Data that you hold



By understanding the types of personal data your organization collects, processes and stores, you can assess the data protection risks and implement appropriate safeguards. This understanding allows you to determine the purposes for which the personal data is used, the legal basis for processing and the rights of individuals whose personal data you handle. It also enables you to establish the RoPA and respond to data subject requests effectively.

A. Performing Data Discovery

Fact:

Organizations of all sizes and sectors can benefit from conducting data discovery to identify personal data they hold, understand data flows, establish the RoPA and assess data protection risks.

Conducting a data discovery exercise allows you to gain a comprehensive understanding of the personal data you collect, process and store. What's more, through conducting a data discovery exercise, you can make more informed decisions about the personal data you process and identify potential vulnerabilities.

▶ Example | Performing Data Discovery

A retail company that operates an online e-commerce platform commences its data protection compliance journey. First, it wants to understand what data it processes. It initiates data discovery by forming a multi-disciplinary team consisting of representatives from IT, legal, compliance and other business units. The team starts identifying and mapping all personal data within the company.

The team takes the following steps:

01 Data Inventory:

The team identifies various data sources, such as customer databases, transaction logs, website analytics and employee records. It also identifies any third-party vendors or partners who process personal data on behalf of the retail company.

02 Data Classification:

The team classifies the types of personal data collected, such as customer names, contact information, purchase history and payment details. It also identifies any sensitive data, such as health data, that requires additional protections under the PDPL.

03 Data Mapping:

The team works closely with its IT teams to trace the flow of data throughout the retail company's systems. It identifies various touchpoints where personal data is collected, processed, and stored, both within internal databases and external systems.

04 Data Purpose and Legal Basis:

The team collaborates with legal and PDPL compliance experts to determine the purposes for which the personal data is collected and the legal basis for such processing.

05 Data Retention and Disposal:

The team identifies any personal data that is no longer necessary for the retail company. It establishes retention periods and implements a process for secure disposal of personal data.

B. Determining a Legal Basis of Processing

Fact:

Consent must meet specific criteria to be considered valid under the PDPL. Consent should be freely given and not obtained through misleading methods. Individuals should have a genuine choice to provide or not provide consent.

Determining a suitable legal basis is the foundation of compliance with the PDPL. By carefully choosing the appropriate legal basis, you can demonstrate a responsible and compliant approach to data protection.

▶ Example | Determining a Legal Basis of Processing

A healthcare provider that offers medical services to its patients collects and processes personal data, including sensitive data such as medical records of its patients.

The healthcare provider takes the following steps:

01 Identifying the Purpose:

The healthcare provider recognizes that to provide quality medical care and manage patient appointments, it needs to process personal data (including sensitive data). It identifies the purpose of processing, which is to fulfill its obligations as a healthcare provider and ensure the well-being of its patients.

02 Selecting the Legal Basis:

After analyzing the purpose of data processing, the healthcare provider determines that the appropriate legal basis is "executing an agreement in which the data subject is a party". This is because the processing of patient personal data is necessary to fulfill its contractual obligation to patients, as it requires the personal data to provide medical services.

03 Informing the Patients:

The healthcare provider informs its patients about the processing activities and the chosen legal basis. It provides clear and transparent information about what personal data will be collected, why it is being processed and how it will be used.

04 Obtaining Consent for Specific Purposes:

While the "executing an agreement in which the data subject is a party" legal basis covers most of the necessary processing for providing medical services, the healthcare provider may still need to process personal data for specific purposes not directly related to the contract, such as sending health-related newsletters and reports. For these additional purposes, the healthcare provider seeks consent from patients.

Please note that if you rely on “Legitimate Interests” as the legal basis of processing, you must undertake a Legitimate Interest Assessment to ensure that it remains an appropriate legal basis for your processing. The requirements for such an assessment are specified in the Implementing Regulations. However, you cannot rely on “Legitimate Interests” as the legal basis if you process sensitive data (e.g., health data).

C. Establishing the Records of Processing Activities (RoPA)

Fact:

Organizations of all sizes and industries must establish the RoPA. Regardless of the scale or nature of your processing, maintaining accurate records is a fundamental requirement under the PDPL.

The RoPA is an explicit requirement under the PDPL. It is a comprehensive inventory of the personal data processing activities conducted by you.

The RoPA also enables you to document data protection risks and appropriate security safeguards to mitigate the data protection risks.

▶ Example | Establishing a RoPA

A technology company offering personalized fitness training programs to its customers has already performed its data discovery.

The technology company takes the following steps:

01 Documentation:

Based on the results of the data discovery, the company carefully documents each processing activity in the RoPA, including the contact details of the controller, the purpose of processing, the categories of personal data involved, the legal basis for processing, information on sharing of personal data within the Kingdom, data retention periods and any data transfers outside the Kingdom.

02 Updates and Maintenance:

The company establishes a process for periodic updates and maintenance of the RoPA. A responsible person, such as the DPO, shall regularly review and update the records, ensuring their accuracy and relevance.

03 Supporting Compliance and Audits:

The established RoPA shall be used for compliance assessments and audits. The company ensures that the records are readily accessible and available for inspection by the competent authority and auditors. This will demonstrate the company’s commitment to compliance with the PDPL.

D. Developing and Publishing Privacy Notices

Fact:

A privacy notice is a living document, and it must be updated when your data privacy practices change.

Developing and publishing privacy notices is a vital practice for organizations to comply with the PDPL. These notices serve as essential communication tools, clearly articulating how personal data is collected, used, and safeguarded. By making privacy notices easily accessible (e.g., on websites and mobile applications), you can empower individuals to make informed decisions about their personal data. The PDPL sets out in detail what information needs to be included in the notices (e.g., the legal basis for collecting personal data, the purpose of collecting personal data, etc.).

▶ Example | Developing and Publishing Privacy Notices

A software company based in Riyadh offers various technology products and services to its customers, including a cloud-based data storage platform. The software company has already established the RoPA. In order to meet its transparency requirements under the PDPL, it decides to create and publish privacy notices for its website and services.

The software company takes the following steps:

01 Drafting Privacy Notices:

The legal team of the company drafts privacy notices that provide clear and concise information about its processing activities. The privacy notices include, for example, sections on data collection, purposes of processing, legal bases, data sharing, data retention periods and individuals’ rights.

02 Accessibility and Language:

Recognizing the importance of accessibility, the company ensures that the privacy notices are easily accessible on its website. The company also provides notices in multiple languages to accommodate its diverse customer base.

03 Publishing Privacy Notices:

The company publishes privacy notices on its website, making them readily available to all visitors and customers. The company also provides direct links to privacy notices during the registration of new users.

04 Periodic Updates:

The company regularly reviews and updates the privacy notices to reflect changes in the company’s processing activities. 3

Section 03

Establishing Accountability and Governance

By implementing a well-defined governance structure, you can effectively manage data protection risks, implement necessary controls and improve data protection compliance in your organization. This will ultimately build trust with individuals and stakeholders who entrust you with their personal data.

A. Assessing the Need for and Appointing a Data Protection Officer (DPO)

Fact:

Under the PDPL, it is not mandatory for all organizations to appoint a DPO. The Implementing Regulations specify the cases when the DPO must be appointed.

By appointing a DPO, you not only comply with the requirements of the PDPL, but also contribute to the successful implementation of your data protection compliance program.

▶ Example | Appointing a DPO

A multinational e-commerce company that operates in the Kingdom processes a significant amount of personal data of its customers (for example. names, addresses, payment information, purchase history, etc.). The company is also involved in regular and continuous monitoring of its customers' internet activity on a large scale. Under the PDPL and Implementing Regulations, it must appoint a DPO.

The e-commerce company takes the following steps:

01 Expertise and Qualifications:

The e-commerce company identifies the necessary qualifications and expertise for the DPO role, such as knowledge of data protection law, data protection practices and risk management.

02 Designation of a DPO:

The company evaluates internal candidates, external professionals and professional organizations providing DPO services with expertise in data protection law.

03 Training and Support:

The e-commerce company provides the DPO with adequate resources, training and support to stay updated on data protection regulations and best practices. The company encourages the DPO to engage in continuous professional development.

04 Communication and Collaboration:

The e-commerce company encourages the DPO to actively communicate and collaborate with different departments, including legal, IT, HR and marketing. The DPO serves as an internal advisor, assisting teams on data protection issues.

B. Establishing a Data Protection Governance Structure

Fact:

Effective governance involves the entire organization and requires a holistic approach that includes accountability mechanisms, policies, procedures and training involving all employees and stakeholders.

A well-defined data protection governance structure establishes the framework for developing and implementing robust policies, procedures and controls that align with the PDPL. This structure should promote transparency, accountability, and a data-protection-centric culture within your organization.

▶ Example | Establishing a Data Protection Governance Structure

A multinational company operating in the technology sector has appointed a DPO. The company is experiencing growing volumes of personal data that it processes. It appreciates the need to establish an effective data protection governance structure to ensure ongoing PDPL compliance.

The DPO takes the following steps:

01 Governance Designation:

The DPO collaborates with the company's senior management to set up a data protection steering committee responsible for overseeing and driving data protection initiatives. The committee comprises representatives from key departments, including legal, IT, HR and marketing. In addition, the DPO defines the structure of the data protection function within the company.

02 Role and Responsibilities:

The DPO outlines the data protection roles and responsibilities of the data protection function. It includes, for example, monitoring compliance with the PDPL, providing guidance on data protection matters and acting as a point of contact for individuals and the competent authority. The DPO shall ensure that data protection considerations are integrated into all business processes and projects. In addition, the DPO manages day-to-day data protection activities, for instance, reviewing the RoPA on a periodic basis.

03 Reporting Structure:

The steering committee, in collaboration with the DPO, ensures that the data protection function operates independently; although this is not stipulated in the PDPL, this is encouraged as best practice for the entity. The company establishes a reporting line that ensures the DPO has autonomy and the necessary authority to carry out the DPO's responsibilities effectively.

04 Data Protection Governance Framework:

The DPO develops a governance framework that outlines roles, responsibilities and reporting lines within the organization. This framework includes clear accountability for data protection compliance and ensures ongoing monitoring, reporting and review of the company's data protection practices.

05 Policy Development:

The DPO, in consultation with the data protection steering committee, develops comprehensive data protection policies and procedures that align with the PDPL. These policies include, for example, personal data handling practices, consent mechanisms, data subject rights, breach notification procedures and vendor risk management.

06 Impact Assessments:

The DPO arranges impact assessments to assess the data protection risks associated, for example, with new projects, systems or processes, or where sensitive data is processed, as well as support in assessing the risks and assisting with mitigation and controls to be implemented. This ensures that data protection considerations are integrated early on in the decision-making process. This approach also reflects the privacy-by-design principles.

07 Monitoring and Auditing:

The DPO establishes processes for monitoring and auditing data processing activities within the company. Regular data protection audits are conducted to identify any gaps or areas of improvement. The results of these audits are used to improve data protection compliance of the organization.

08 Training and Awareness:

The DPO designs and implements data protection training programs for the company's employees at all levels. These programs educate staff members on their data protection responsibilities as per the PDPL and the company's policies. Training sessions are conducted regularly to keep employees informed about evolving data protection requirements.

09 Stakeholder Engagement:

The DPO facilitates regular communication and collaboration with internal stakeholders, including senior management, department heads and employees, to create a culture of data protection awareness.

C. Developing Policies, Procedures and Conducting Training

Fact:

Policies and procedures require ongoing review and updates to align with changing data protection regulations, best practices and organizational needs.

Policies and procedures, when developed correctly, provide clear guidelines on how personal data should be processed within your organization. These policies and procedures serve as a roadmap for your employees, guiding them on how to mitigate data protection risks.

▶ Example | Developing Policies and Procedures

A financial institution processes a large amount of personal data. To ensure ongoing compliance with the PDPL, the financial institution decides to develop comprehensive policies and procedures for data protection.

The financial institution takes the following steps:

01 Data Protection Policy:

The financial institution develops an internal data protection policy in which it specifies general rules on how it processes personal data. The policy

covers areas such as data protection strategy, data protection principles, data protection governance in the organization, etc.

02 Policies and Procedures related to specific data protection areas:

The financial institution establishes policies and procedures for various personal data processes, including data subject request policy and procedure; impact assessment policy and procedure; data protection by design and by default policy; policy for monitoring and oversight of third parties; personal data breach response policy and procedure; consent management procedure data retention policy. The policies and procedures ensure that all the employees process personal data in one uniform way across the whole organization.

03 Complaints and Data Subject Requests:

The financial institution implements a process for the management of complaints and data subject requests. The process outlines the steps for receiving, verifying, responding to, and documenting complaints and data subject requests.

04 Vendor and Third-Party Management:

The financial institution establishes procedures for managing the data protection risks arising from third parties, including vendors and service providers that have access to personal data. The procedures include conducting due diligence assessments (including by using a data protection procurement questionnaire), defining contractual obligations regarding data protection and ongoing monitoring of third-party compliance through periodic audits.

05 Personal Data Incident Response Plan:

The financial institution develops an incident response plan that outlines the steps to be taken in the event of a personal data breach or incident. The plan includes procedures for incident identification, containment, notification to the competent authority and data subjects (where required) and coordination with relevant internal and external stakeholders, such as the competent authority and affected data subjects.

D. Implementing Processes for Data Subject Rights Requests

Fact:

Individuals have the legal right under the PDPL to revoke their consent for processing, after which organizations must stop such processing without undue delay.

Respecting individual rights builds trust between you and the individuals whose personal data you process. In addition to compliance with the PDPL, by upholding data subject rights, you can strengthen your reputation as a responsible data controller in the Kingdom's data-driven landscape.

▶ Example | Implementing Processes for Data Subject Rights Requests

An e-commerce company that sells eco-friendly products to customers worldwide has implemented a data protection compliance program that includes handling data subject rights requests.

One of the customers sends an email to the company's online store requesting access to her personal data held by the company. She wants to know what information is stored and how it is being used.

The DPO takes the following steps:

01 Prompt Response:

Upon receiving the request, the DPO acknowledges the request and informs the customer that her request is being processed.

02 Data Verification:

The DPO verifies the customer's identity to ensure that the request comes from the actual data subject (e.g., by sending her a verification code).

03 Data Compilation:

The DPO collaborates with relevant departments within the e-commerce company to compile the requested personal data in a clear and understandable format.

04 Providing the Information:

The company provides the customer with access to her requested personal data, including the categories of processed data, the purposes of processing and any third parties with whom her personal data is shared.

05 Rectification Request:

After reviewing the provided data, the customer realizes that her address is outdated. She sends another email to the company, requesting a correction of her address.

06 Timely Correction:

The company promptly updates the individual's address in its records and informs her of the correction made.

07 Consent Withdrawal and Erasure:

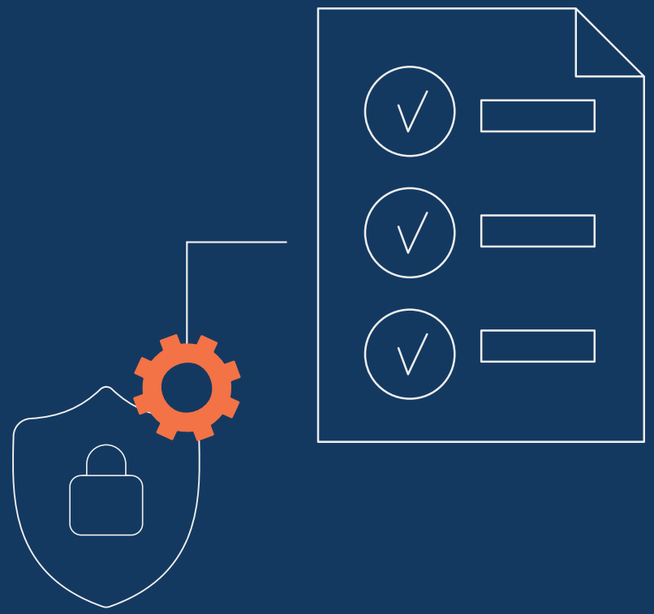
A few months later, the customer decides that she no longer wishes to be associated with a specific marketing campaign. She withdraws her consent and requests the deletion of her data related to that campaign.

08 Ceasing Processing and Complying with Erasure:

The company reviews the customer's request, stops processing the personal data and erases the personal data, as requested.

Section 04

Conducting Impact Assessments



Fact:

Impact Assessments are a vital tool for identifying and mitigating data protection risks associated with personal data processing.

An impact assessment is a systematic process used to assess and manage data protection risks associated with data processing activities. It involves identifying and evaluating potential data protection risks and implementing measures to mitigate those risks. Impact assessments are important because they enable you to proactively identify and address data protection risks, protect data subjects' rights and demonstrate accountability in your data processing practices.

How do I conduct an Impact Assessment?

SDAIA has a simple and straightforward impact assessment service that is designed to assess the data protection risks associated with your intended processing. This service allows you to make informed decisions about data protection risk mitigations to reduce the risk of the intended processing. For conducting an impact assessment, please visit the National Data Governance Platform. Specific requirements for the impact assessments are defined and set out in the Implementing Regulations.

▶ Example | Conducting Impact Assessments

A software development company operating in the Kingdom plans to launch a new software-based technology that collects and analyzes personal data from different sources for targeted advertising. Recognizing the technology's potential data protection risks to individuals and the requirement of the PDPL, the software company decides to conduct an impact assessment.

The software development company takes the following steps:

01 Scope and Objectives:

The software company defines the scope of the impact assessment, identifying the specific features and functionalities of the technology that require assessment.

02 Data Processing Activities:

The software company conducts a comprehensive inventory of the data processing activities associated with the technology. It documents the types of personal data collected, the purposes of data processing, the legal basis for processing and any data sharing or third-party involvement.

03 Risk Assessment and Mitigation:

The software company assesses the data protection risks associated with the technology by considering factors such as the sensitivity of the data collected, potential data breaches, impact on individuals' rights, the principles of the PDPL, the necessity and

proportionality of the processing and the current state of the technology. It identifies potential risks, such as unauthorized access to personal data and excessive data retention periods.

Based on the identified risks, the software company develops a set of actions to mitigate the identified risks and ensure that the technology is developed in line with privacy-by-design principles. This may include implementing encryption mechanisms, incorporating data protection settings and consent mechanisms, conducting regular security assessments and providing clear and transparent privacy notices.

04 Consultation and Stakeholder Engagement:

The software company engages relevant stakeholders, such as data protection and software development experts, to gather feedback and ensure that the impact assessment adequately addresses the data protection risks. It considers the perspectives of individuals whose personal data is being processed, internal teams responsible for the technology's development and maintenance and external partners involved in the data processing.

05 Documentation and Decision Making:

The software company documents the impact assessment, including its findings, recommendations and the decisions made based on the assessment. It ensures that the impact assessment report is available for review by the competent authority or other relevant entities.

06 Review and Iteration:

The software company recognizes that the impact assessment is not a one-time activity and commits to reviewing and updating it periodically or whenever significant changes are made to the technology. It establishes a process for ongoing monitoring, evaluation and improvement of data protection practices in line with the assessment's findings and recommendations.

Section 05

Privacy by Design and Default

Fact:

It is more efficient and cost-effective to address data protection considerations early in the development process rather than attempting to implement data protection measures later.

Privacy by Design and Default, although not strictly required under the PDPL, is strongly encouraged to be embedded into all stages of your personal data processing lifecycle. Implementing privacy by design and default means integrating data protection considerations at every stage of your organization's processes, products and services. It involves proactively addressing data protection risks from the outset and adopting data protection-friendly practices. This approach builds trust with users and ensures ongoing compliance with the PDPL.

▶ Example | Implementing Privacy by Design and Default

A large medical center that is based in the Kingdom is developing an online patient portal to provide convenient access to medical records and appointment scheduling for its patients. In addition, it aims to act as a research platform for doctors to conduct research on the illnesses that are affecting the Kingdom's population. The medical center decides to implement privacy by design and default principles in the development of its patient portal.

The medical center takes the following steps:

01 Data Access Controls:

During the development of the patient portal, the medical center incorporates strict access controls to ensure that only authorized healthcare professionals can access patient records. This includes role-based access permissions and multi-factor authentication.

02 Privacy-Centered User Interface:

The medical center designs the patient portal with data protection in mind, ensuring that sensitive health data is not displayed publicly or visible to unauthorized users. The portal only reveals relevant health data to individual patients when they log in securely.

03 Consent Management:

In compliance with the PDPL, the medical center implements a consent management system. Patients are explicitly informed about the data processing activities and asked for their consent before any personal data is collected, shared or used.

04 Data Anonymization:

For research purposes, the medical center anonymizes patient data. This allows them and other doctors to perform valuable research on population health while preserving patient's privacy.

05 Data Encryption:

The medical center ensures that all data, at rest and when being transmitted between the patient portal and its systems, is encrypted. This practice reduces the risk of unauthorized access during data transmission and when data is at rest. The medical center will also use pseudonymization controls where applicable.

06 Regular Data Protection Audits:

Throughout the development process and after the patient portal's launch, the medical center conducts regular data protection audits to assess ongoing compliance with the PDPL's requirements and identifies areas for improvement. These audits help them stay proactive in addressing data protection risks.

07 Data Protection Training:

The portal development team and medical staff undergo data protection training to understand the importance of privacy by design and default principles. They learn how to handle patient data in compliance with the PDPL.

Section 06

Implementing Personal Data Breach Handling Procedure

Fact:

A personal data breach must be reported in cases determined by the Implementing Regulations.

Implementing personal data breach handling procedures is crucial for effective data protection compliance within your organization. These procedures enable you to respond promptly and appropriately in the event of a personal data breach in compliance with the PDPL. By having a clear and well-defined breach handling procedure, you can mitigate the consequences of a data breach in an efficient manner.

▶ Example | Implementing Personal Data Breach Handling Procedure

A financial institution that processes a large amount of personal data, including customers' credit data, recognizes the need for a personal data breach handling procedure.

The financial institution takes the following steps:

Establishing Incident Response Team:

The financial institution forms a dedicated incident response team consisting of representatives from IT, legal, compliance and external communication departments. This team is responsible for managing any suspected or confirmed data breaches.

01 Breach Detection and Assessment:

The incident response team implements monitoring and detection measures to identify potential data breaches promptly. In the event of a suspected breach, it conducts a rapid assessment to determine the nature and scope of the incident.

02 Incident Classification:

Based on the assessment, the incident response team classifies the breach according to its severity. It considers factors such as the type of data compromised, the number of affected individuals and the potential harm that may arise.

03 Notifying the competent authority:

If the incident potentially causes or leads to harm to the personal data or to the data subject or conflicts with their rights or interests, the financial institution promptly notifies the competent authority. The incident response team ensures that all necessary details are included in the notification.

04 Notifying Affected Individuals:

The financial institution shall notify individuals affected if the breach may cause damage to their data or conflict with their rights or interests.

05 Coordination with Relevant Competent Authorities:

If the personal data breach involves criminal activity, the incident response team collaborates with relevant competent authorities to investigate the incident and to take necessary legal actions.

06 Incident Documentation and Analysis:

The incident response team thoroughly documents all actions taken during the breach response process. They conduct a post-incident analysis to identify lessons learned and implement necessary improvements to prevent similar incidents in the future.

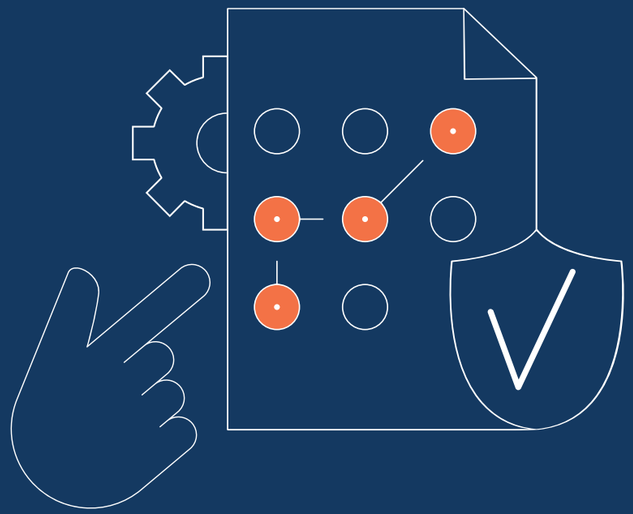
The company may need to make breach notifications to other regulators or bodies, as applicable.

How do I notify the competent authority of a personal data breach?

If you suspect that a personal data breach has taken place within your organization, it is critical that you comply with the requirements to report the personal data breach, as such requirements are specified in the PDPL and Implementing Regulations. The NDMO has a simple and straightforward personal data breach reporting form that is designed to minimize the time spent on personal data breach reporting. For reporting a personal data breach, please visit the National Data Governance Platform.

Section 07

Implementing Technical and Organizational Measures



Fact:

Technical and organizational measures include more than just cybersecurity measures.

Technical and organizational measures are essential components of any effective data protection program. Technical measures include cybersecurity controls and technologies, such as data encryption, access controls and intrusion detection systems. Organizational measures involve policies, procedures and training to ensure employees and stakeholders understand their responsibilities and follow data protection best practices.

▶ Example | Implementing Technical and Organizational Measures

A technology company that provides cloud-based data storage and IT services to various clients, including businesses and government agencies, has implemented the below technical and organizational measures to safeguard the personal data they handle.

The company takes the following steps:

01 Data Encryption:

The company employs data encryption protocols to ensure that all personal data stored and transmitted through its cloud services is securely protected.

02 Logical Access Controls:

To restrict data access to authorized personnel only, the company implements strict logical access controls. Employees are granted access based on their roles, and multi-factor authentication is employed to strengthen security.

03 Physical Access Controls:

To restrict physical access to its data centers, the company implements CCTVs, security lighting and alarms, visitor logs, ID badges and other strict physical measures that secure the data centers from unauthorized access.

04 Cybersecurity Controls:

The company implements strong cybersecurity controls such as firewalls, periodic malware scans and anti-virus protection to reduce the likelihood of personal data leakage and to identify vulnerabilities.

05 Employee Training:

The company conducts regular data protection and security training for all employees. Staff members are educated on data handling best practices, data protection policies and potential security threats.

06 Incident Response Plan:

As part of its policies and procedures suite, the company has developed an incident response plan that outlines the procedures to be followed in the event of a data breach or security incident.

07 Data Minimization:

As part of its privacy-by-design framework, the company practices the principle of data minimization in its processing. It only collects and retains the personal data necessary for the provision of its services, reducing the risk associated with excessive data storage.

08 Vendor Management:

The company collaborates with third-party vendors and subcontractors to fulfill its cloud service offering to its clients. To ensure data protection compliance throughout the supply chain, the company establishes stringent contractual requirements regarding data protection and security measures.

Section 08

Sharing Personal Data within the Kingdom

Fact:

Even when personal data is transferred within the Kingdom, you must still adhere to the PDPL's requirements and adopt appropriate technical and organizational measures.

By sharing personal data within the Kingdom responsibly and transparently, you can ensure that your data subject's personal data remains protected and used only for authorized purposes.

▶ Example | Transferring Personal Data within the Kingdom

A bank operating within the Kingdom provides various financial services to its customers, including account management, loans and investments. As part of its operations, the bank collects and processes the personal data of its clients and shares it with a third-party processor.

The bank takes the following steps:

01 Customer Data Processing:

The bank collects and processes the personal data of its customers, including names, addresses, financial transactions and credit histories. This personal data is used to provide banking services, manage accounts and assess creditworthiness.

02 External Data Sharing:

To facilitate seamless customer service and operation of the customer's bank account, the bank shares certain customer's personal data with a third party for KYC measures.

03 Legal and Compliance Review:

Before sharing customer data with the third-party processor, the bank reviews the data sharing practices under the PDPL and Implementing Regulations to ensure the necessary safeguards are in place, for example, that the processor has provided necessary safeguards for the personal data, there is monitoring in place between the parties, a lawful basis has been determined for the disclosure, etc.

04 Deletion or Return of the Personal Data:

Once the processing by the processor is completed, the personal data is deleted or returned to the bank.

05 Access Controls:

The bank implements strict access controls within its internal systems. Employees are granted access only to the personal data necessary for their respective roles, minimizing the risk of unauthorized access and ensuring data security.

06 Employee Training:

To ensure awareness of the lawful handling of customer personal data, the bank conducts regular data protection and security training for its employees regarding the disclosure of personal data.

07 Transparent Communication:

The bank includes information about personal data-sharing practices in its privacy notice. Customers are informed about the purpose of data sharing, the departments involved and the safeguards in place to protect their personal data.

08 Continuous Monitoring:

The bank regularly monitors its data-sharing processes with the third party to ensure that access controls are effective and the personal data is being used only for documented purposes. Any unauthorized access attempts or suspicious activities are promptly reported to them.

Section 09

Transferring Personal Data outside the Kingdom

Fact:

Transfers outside the Kingdom are subject to additional requirements under the PDPL and Implementing Regulations.

Transferring personal data outside the Kingdom involves moving individuals' personal data from the Kingdom to another country or jurisdiction. This process is often necessary for global business operations, partnerships or service delivery (e.g., while using cloud storage solutions). Such arrangements are subject to specified requirements of the PDPL and Implementing Regulations.

▶ Example | Transferring Personal Data outside the Kingdom

A multinational technology company headquartered in a foreign jurisdiction (a non-adequate jurisdiction[3]) offers software solutions and IT services to clients around the world, including in the Kingdom. As part of its global operations, the company collects and processes personal data from clients, employees and partners.

The company takes the following steps[4]:

01 International Client Engagement:

The company secures a contract with a client based in the Kingdom to provide customized software development services. The client provides the personal data of its employees for account set-up and project management.

02 Data Transfer Necessity:

To efficiently deliver services to its client, the company needs to share certain personal data of Saudi residents, including employee names and contact information, with its development teams located in foreign jurisdictions. Therefore, the company makes a decision to arrange the transfer of personal data outside of the Kingdom.

Since the transfer is to a non-adequate jurisdiction, the company will need to review Art. 29 of the PDPL and the General Provisions of the implementing Regulations to ensure, amongst other things, the following:

- whether the transfer will impact national security or vital interests of the Kingdom;
- whether only the minimal amount of personal data necessary to fulfill the processing should be transferred;
- whether the rights of data subjects are taken into account;
- whether the purpose for the transfer has been established;
- whether an appropriate safeguard has been put in place, e.g., Binding Common Rules, standard contractual clauses, etc.; and
- Whether a risk assessment has been undertaken.

03 Privacy Notices and Transparency:

Both the company and its client update their privacy notices to inform their respective stakeholders about the cross-border data transfer, including the legal bases and safeguards in place.

04 Data Retention:

Once the engagement is completed, the company securely deletes any personal data transferred, as per the conditions of the data sharing agreement.

[3] Non-adequate jurisdiction means jurisdiction that is not on the list of jurisdictions that have an adequate level of protection for Personal Data outside the Kingdom. Such list shall be adopted in the Kingdom.

[4] Please note this is a very high-level step plan. The detailed review of the PDPL and Implementing Regulations will need to be undertaken to ensure compliance with cross-border personal data transfer requirements.

Section 10

Monitoring and Auditing Compliance

Fact:

Monitoring and auditing compliance is an ongoing process that should be conducted regularly to ensure ongoing compliance with the PDPL.

Monitoring and auditing compliance is a vital aspect of effective data protection compliance within your organization. It involves ongoing assessments to ensure adherence to the PDPL and internal data protection policies. Regular monitoring helps detect potential data protection risks and weaknesses in data protection practices, while audits provide a comprehensive evaluation of the organization's data protection compliance program. By continuously monitoring and auditing compliance, you can proactively address any issues, implement necessary improvements and demonstrate a commitment to compliance with the PDPL.

▶ Example | Monitoring and Auditing Compliance

A popular luxury hotel handles a vast amount of guest data, including personal data, payment details and preferences. To maintain a high standard of protection and to comply with the PDPL, the hotel implements a robust monitoring and auditing program.

The hotel takes the following steps:

01 Ongoing Monitoring:

The hotel conducts regular internal monitoring to ensure that its staff follows the established data protection policies and procedures. The management team periodically reviews access controls and data handling practices to identify any potential compliance issues.

02 Regulatory Watch:

The hotel's legal function closely tracks updates from relevant data protection regulatory bodies while also staying informed about court rulings and international agreements impacting data protection.

03 Incident Monitoring:

The hotel employs a system to monitor for any potential data breaches or data protection incidents. The monitoring system alerts the data protection officer and the incident response team in real-time if any unusual activities are detected.

04 External Audits:

The hotel contracts a third-party data protection auditor to conduct regular audits of its data protection compliance program. The external auditor assesses the effectiveness of data protection controls, data processing practices and adherence to the PDPL's requirements.

05 Guest Data Access Logs:

The hotel maintains access logs to track employee access to guest data. This log helps monitor and detect any unauthorized access or potential personal data breaches.

06 Incident Response Testing:

To ensure readiness in the event of a personal data breach or security incident, the hotel periodically conducts incident response testing. This involves simulating various scenarios to evaluate the

effectiveness of its response procedures.

07 Supplier Management:

Being in the hospitality sector, the hotel relies on various suppliers and partners to fulfill services. The hotel implements a supplier management program that includes data protection requirements in contracts and conducts periodic audits of suppliers' data protection practices to ensure compliance.

What resources do you have for ongoing compliance?

The NDMO has a simple and straightforward compliance assessment service that is designed to highlight areas of focus in your organization's data protection compliance program. To access this service, please visit the compliance assessment service on the National Data Governance Platform.

To read the full law and the implementing regulations please visit SDAIA's website

National Data Governance Platform