SDAIA
الهيئة السعودية للبيانات
والذكاء الاصطناعي
Saudi Data & AI Authority

Guide to the Saudi Personal Data Protection Law

For Controllers and Processors

Version 1.0

December 2023

Table of Contents

Introduction 3

- Purpose 3
- Aim 3

Data protection in the Kingdom of Saudi Arabia 4

- Scope of the PDPL 4
- Material scope: What does PDPL regulate? 5
- What is personal data? 5
- How can individuals be identified? 6
- What is sensitive data? 8
- What are the specific provisions regarding processing sensitive data? 8
- What forms can personal data take? 9
- What are the sources of personal data? 9
- Are opinions and inferences of individuals considered personal data? 10
- Processing data of a deceased individual 10
- Is pseudonymized data considered personal data? 11
- Is anonymized data considered personal data? 13
- What is meant by processing of personal data? 13

Territorial scope: Where does the PDPL apply? 15

- Scenario 1: What is considered as processing in the Kingdom? 15
- Scenario 2: Who are considered as individuals residing in the Kingdom? 16
- Scenario 3: Who are considered as parties outside the Kingdom? 17

What roles do controllers and processors play under the PDPL? 18

When does the PDPL not apply? 19

- What is personal or family use? 19

When will the PDPL come into force? 20

- What should you do during the grace period? 20

Who is the Competent Authority? 21

Individuals' rights 22

Data protection principles 23

Appendix 1 - Non-exhaustive list of examples of bad data protection practices 25

Introduction

Purpose

The purpose of this document ("**Guidance**") is to introduce you to the Personal Data Protection Law of Saudi Arabia ("**PDPL**"), approved by the Royal Decree No. 19/m, dated 1443/2/9, and to explain how the PDPL will apply.

Aim

The aim of the Guidance is to clarify the PDPL and provide directions to individuals and organizations for compliance with the PDPL. The Guidance does not contain any binding rules or obligations. It does not have the status of a law or a similar legal instrument in the Kingdom.

Data protection in the Kingdom of Saudi Arabia

Establishing a thriving digital economy is one of the key priorities for the Kingdom of Saudi Arabia (**"Kingdom"**) as per the Saudi Vision 2030. Data is the foundation of the modern digital economy. Therefore, it is essential that the use of personal data (including data privacy) is regulated in the Kingdom.

The data protection regulatory framework in the Kingdom includes the following:

1. the PDPL;
2. the Implementing Regulations to the PDPL, including the Implementing Regulation to the PDPL and Regulation on Personal Data Transfer outside the Kingdom;
3. Regulations, standards, policies and other legal instruments in the data protection area issued by the Saudi Data and AI Authority (**"SDAIA"**);
4. International treaties in the data protection area to which the Kingdom may be a party.

The PDPL is the key law in the Kingdom in the area of personal data protection. If you use personal data, you must always comply with the PDPL. You could be exempted from an obligation to comply with the PDPL in limited cases in accordance with the legal instruments issued by the competent authorities in the Kingdom.

For more details on the competent authority in the area of personal data protection (**"Competent Authority"**), please see section "Who is the Competent Authority?" of this Guidance.

Scope of the PDPL

The PDPL has the following scope.

Article 2 of the PDPL

1. The Law applies to any Processing of Personal Data related to individuals that takes place in the Kingdom by any means, including the Processing of Personal Data related to individuals residing in the Kingdom by any means from any party outside the Kingdom. This includes the data of the deceased if it would lead to them or a member of their family being identified specifically.

2. The scope of applying the Law excludes the individual›s Personal Data Processing for purposes that do not go beyond personal or family use, as long as the Data Subject did not publish or disclose it to others. The Regulations shall define personal and family use provided in this Paragraph.

Material scope: What does PDPL regulate?

The PDPL regulates the processing of personal data. It includes regulation of processing of:

1. personal data of any type, including sensitive data;
2. personal data from any source and in any form;
3. pseudonymized data;
4. data of deceased (in some cases).

What is personal data?

The PDPL has the following definition of personal data.

Article 1(4) of the PDPL

Any data, regardless of its source or form, that may lead to identifying an individual specifically, or that may directly or indirectly make it possible to identify an individual, including name, personal identification number, addresses, contact numbers, license numbers, records, personal assets, bank and credit card numbers, photos and videos of an individual, and any other data of personal nature.

This means that personal data is any data based on which it is possible to identify an individual, for example an individual's telephone number, name or email address.

If it is impossible to identify a particular individual from the data in question, then such data is not personal data and its use is not regulated by the PDPL.

Example | Personal data

An organization's HR department stores data about each employee, including name, date of birth, job grade, personal phone number and educational qualifications. This data is considered personal data and its use is regulated by the PDPL.

Example | Non-personal data

A company›s marketing department analyzes the purchase behavior of its customers between the ages of 20 and 30 for analytics purposes. The marketing department only has data about the products and the price of items purchased by this age group. The marketing department is unable to identify any individual purchaser.

Therefore, such data is not personal data. Its use is not regulated by the PDPL.

Example | Non-personal data

An automotive company has a database of its authorized dealerships (commercial organizations). The database has data on how many cars each dealership sold during the last year. The database also contains prices for which the dealerships purchase the cars for further resale.

The data on the volume of sales and the price of cars is not personal data. Its use is not regulated by the PDPL.

How can individuals be identified?

You may identify an individual:

1. **Directly** – based on the data you are processing, for example unique identifiers such as a personal telephone number, name or personal email address. Processing of such data is in the scope of the PDPL.
2. **Indirectly** - based on the data from several databases, if such databases could be linked with each other and, as a result, an individual could be identified. In such cases, the data in these separate databases shall be considered personal data. Its use shall be regulated by the PDPL. However, if linking the databases cannot lead to identification of the individual, then the data from such databases would not be considered personal data. It would be outside the scope of the PDPL.

Please note that you must consider each case separately to understand if under given circumstances it is possible to identify an individual.

Example | Personal data | Directly identifying an individual

A retail store collects the phone numbers of each customer before selling products to them. This is done in order to send customers text messages about new sales offers. The retail store does not collect the names of its customers.

...

Example | Personal data | Directly identifying an individual

The phone numbers are linked to the names of specific customers in the database of the telecommunication provider. Therefore, the phone numbers will be considered personal data for the telecommunication provider.

The phone numbers will be considered personal data for the retail store as well – even if the store does not have access to the database of the telecommunication provider. This is because each phone number is assigned uniquely to one individual, the retail company can single out the individual from all other customers based on his phone number and may use such a phone number to contact the individual and address sales offers particularly to him.

Therefore, both the retail store and the telecommunication provider will need to protect the phone numbers in accordance with the PDPL.

Example | Personal data | Indirectly identifying an individual

A company's physical security department stores the following data in two separate databases in separate systems:

Database 1: this database contains names, phone numbers and employee IDs, which are used for identity and for payroll management;

Database 2: this database contains data on the vehicles that entered and exited the company premises. Such database is used to issue warnings for parking violations.

In this case, Database 1 stores data that can directly identify an individual and thus contains personal data.

While Database 2 does not store data that can directly identify an individual, the company is able to link the two databases together to identify the owner of a vehicle. Thus, the data in Database 2 should also be considered personal data. Its use will be regulated by the PDPL.

Example | Personal data | An individual cannot be identified

A pharmacy decided to analyze its commercial data for the previous year. Before doing an analysis, it irrecoverably deleted from the purchase history the data that could be linked to particular individuals, including phone numbers and bank card numbers.

After such deletion, the pharmacy only had the following data:

1. The name and type of the product.
2. The details of the items of the products sold during the previous year.
3. The price for which the product was sold.

The above data in the dataset is not considered personal data. Its use will not be regulated by the PDPL.

What is sensitive data?

Under the PDPL, there is a separate subset of personal data referred to as “sensitive data”. This type of data requires additional safeguards and protections as the unauthorized access of such data may cause serious harm to the individual.

Sensitive data includes the following:

1. Personal data that reveals the racial or ethnic origin of an individual (e.g., skin color of an individual, etc.);
2. Personal data that reveals the religious, philosophical (intellectual) or political beliefs of an individual;
3. Personal data that reveals any prior criminal convictions and/or offenses of an individual;
4. Biometric data of an individual (where used for identification purposes);
5. Genetic data of an individual;
6. Personal data that is related to the health of an individual; and
7. Personal data that reveals whether the parentage (either one or both parents) of the individual is unknown.

What are the specific provisions regarding processing sensitive data?

When processing sensitive data, you must comply with all the requirements of the PDPL that are applicable to processing of any other personal data.

That said, please note that the PDPL has specific requirements for processing of sensitive data, for example:

1. You may not use legitimate interest as a lawful basis when processing personal data (as per Art. 6 (4) of the PDPL).
2. If you rely on consent as a lawful basis for processing of sensitive data, such consent must be explicit (as per Art. 11 of the Implementing Regulation to the PDPL).
3. In all circumstances, even with an individual’s consent, you may not process sensitive data for marketing purposes (as per Art. 26 of the PDPL).
4. PDPL provides for restrictions on the use of non-anonymized sensitive data for scientific, research, or statistical purposes (as per Art. 27 of the PDPL).

What forms can personal data take?

PDPL regulates processing of personal data in all forms.

Personal data in non-electronic form (such as personal data in a physical document) also falls within the scope of the PDPL. In practice, given the level of technological advancement in the Kingdom, the majority of processing will relate to personal data in electronic form.

Example | Personal data | Personal data in electronic form

HR department stores personal data about employees of the organization in several cloud storage systems. Such personal data exists in electronic form. Its use is regulated by the PDPL.

Example | Personal data | Personal data in non-electronic form

A university stores exam papers of its students. The exam papers contain personal data of students (for example, full names and ID numbers). Such personal data exists in non-electronic form. Its use is regulated by the PDPL.

The PDPL applies to the processing of personal data irrespective of the volume or type of personal data being processed. This means that small and medium-sized businesses are also subject to compliance with the PDPL.

In addition, the PDPL does not differentiate between other forms of personal data such as structured data (e.g. the data stored in databases) or unstructured data (e.g. personal data in different documents). As long as the data can identify a specific individual, it is considered as personal data and its use is regulated by the PDPL.

What are the sources of personal data?

You may obtain personal data from various sources including directly from the individual or from other parties, e.g. from public sources (e.g. from publicly open internet databases). The PDPL determines in its Art. 10 specific conditions for obtaining personal data from sources other than the data subject directly.

Are opinions and inferences of individuals considered personal data?

Personal data can also include opinions and inferences if an individual can be directly or indirectly identified from them. If an organization attaches opinions or inferences to an individual then, no matter whether such opinions or inferences are correct, they are likely to be considered personal data.

Example | Personal data | Opinions

An HR department conducts a survey regarding the satisfaction of employees with the work environment. Based on this survey, the HR department prepares a report on how the work environment could be improved.
In this case, the opinions of the employees will be considered as personal data.

Example | Personal data | Inferences

A pharmacy has a database with a purchase history of its customers. The database links specific customers to the medicines that they have purchased.

Based on the purchase history, the pharmacy makes inferences about the health conditions of its customers and based on such inferences it conducts analytics.

The inferences that the pharmacy makes about the health conditions of their customers will be considered personal data. It will be considered sensitive data even if some customers did not buy medicines for themselves (for example, they bought medicals for their relatives).

Note: In this example, a customer database is maintained on the purchasing history of the individual. The pharmacy is not able to differentiate between purchases that customers make for themselves or others.

Processing data of a deceased individual

Pursuant to Art. 2 (1) of the PDPL

The processing of a deceased person's data is also in the scope of the PDPL if such pro-cessing would lead to them or a member of their family being identified specifically.

This provision of the PDPL does not mean that the use of the data of a deceased person is always subject to the same requirements as the personal data of a living individual. Instead, it means that if the data of a deceased individual may cause harm to an identified living family member (for example, reputational harm), then such data of a deceased individual must be protected in the same way as the personal data of a living individual.

What is considered harm to an identified living individual and what exact PDPL requirements should apply to the deceased person's data must be considered in each particular case.

Example | Personal data | Data of the deceased

A company offers a service to research an individual's family history. In undertaking this research, the company identified that the deceased father of the individual suffered from a dangerous infectious disease. The individual who has ordered the research considers that this information may cause harm to his reputation. The individual notifies the research company about this fact and explains to them the reasons for this opinion.

In such case, the data of the deceased father will need to be protected by the research company in the same way as if it was personal data of the living individual.

Is pseudonymized data considered personal data?

The Implementing Regulation to the PDPL provides for a definition of the "pseudonymization":

Article 1 (7) of Implementing Regulation to the PDPL

Conversion of the main identifiers that indicate the identity of the Data Subject into codes that make it difficult to directly identify them without using additional data or information. The pseudonymized data or additional information should be kept separately, and appropriate technical and administrative controls should be implemented to ensure that they are not specifically linked to the data subject›s identity.

Pseudonymization is a technique that replaces or removes data in a dataset that directly identifies an individual. Pseudonymized data is still considered personal data and acts as an effective data security measure. Pseudonymization involves masking identifying data, for example by replacing directly identifying data (such as names) with a unique identifier. Such an identifier can no longer be attributed to a particular individual without the use of additional data.

Pseudonymization is a data protection and security-enhancing measure that assists with risk mitigation. It is used in a number of areas, for example, clinical trials and medical research, financial sector, etc.

Example | Pseudonymization | Banking services

A bank wants to provide special offers to its customers. The offers depend on the customers' volume of transactions.

The bank took the following steps.

1. It separated the names of customers from their transactions into two separate databases:
   - the first database contains names of the customers;
   - the second database contains the volumes of their transactions;
   - the names of the customers were replaced with symbols in the second database.
2. These two separate databases were provided to two separate teams in the bank for analysis.
3. Each team held its own passwords to the database. One team could not access the database of the other team.

Therefore, the bank pseudonymized the data of its customers.

In this case, the data on volumes of transactions will be considered personal data. This is because:

- it will be possible to link volumes of transactions to particular customers, if both databases are combined;
- both databases are kept within the same bank and the bank has a real possibility to combine such databases when required.

Example | Pseudonymization | Educational sector

A university maintains a database with data of its students. In this database, each student has his/her own unique ID number.

When undertaking their exams, students are required to specify in the exam papers their ID number only. When the exam board reviews the exam papers, the exam board can only see the ID number of each student. The exam board does not know the name of the student who took the exam. The exam board does not have access to the database where the ID numbers are matched with the names of the students.

Therefore, the university in this case pseudonymized the names of the students.

The ID numbers of students will still be considered as personal data. This is because the university may match in its database the ID numbers with names of the students.

Is anonymized data considered personal data?

Article 1 (8) of Implementing Regulation to the PDPL

Removal of direct and indirect identifiers that indicate the identity of the Data Subject in a way that permanently makes it impossible to identify the Data Subject.

Anonymization is the process of removing any personally identifiable information from a data set so that you are no longer able to identify an individual in any way. As such, anonymized data is not considered personal data. Its use is not regulated by the PDPL.

Therefore:

1. The personal data which underwent anonymization is no longer subject to the PDPL.
2. The individuals cannot exercise the rights, as specified in the PDPL, in relation to the use of their anonymized personal data.

When done correctly, anonymization eliminates the data protection risks. This is because anonymized data cannot directly or indirectly identify the individual. Art. 9 of the Implementing Regulation to the PDPL specifies certain requirements for anonymization.

Please note, however, that the process of anonymizing personal data is still considered processing of personal data. Thus, it is subject to the scope and provisions of the PDPL.

What is meant by processing of personal data?

The PDPL has the following definition of processing of personal data.

Article 1 (5) of the PDPL

Any operation carried out on personal data by any means, whether manual or automated, including collecting, recording, saving, indexing, organizing, formatting, storing, modifying, updating, consolidating, retrieving, using, disclosing, transmitting, publishing, sharing, linking, blocking, erasing and destroying data.

Processing is taking any action on personal data. For example, even if you only hold personal data (store personal data), you will be considered as processing it - even if no further action is taken on it.

In essence, this means that any use of personal data is considered processing of personal data. Its use is subject to the provisions of the PDPL.

Example | Processing of personal data | Personal data collection

An online store requires customers to register on its website to purchase products. The customers have to specify their names, emails, logins, passwords and delivery addresses.

When the customer provides the above personal data to the website, it is considered to be collected by the online store.

Example | Processing of personal data | Personal data storage

A manufacturing company has a large database of all its employees. The database includes the personal data of employees, including their names, contact information and education qualifications. The company has contracted a cloud service provider to store the database of the employees in the cloud.

Storage of such personal data in the cloud is processing of personal data. It is regulated by the PDPL.

You must ensure that processing is conducted in a manner that is fair, lawful, and transparent and in accordance with the principles of the PDPL. For more information on the principles of the PDPL, please see the section “Data protection principles” of this Guidance.

Territorial scope: Where does the PDPL apply?

The territorial scope is the territorial area where the PDPL applies.

The territorial scope of the PDPL includes processing in two scenarios:

Scenario 1: processing of personal data in the Kingdom by any means.

Scenario 2: processing of personal data of individuals who reside (stay) in the Kingdom by any means from any party, including the party located outside the Kingdom.

Scenario 1: What is considered as processing in the Kingdom?

The PDPL applies to processing of personal data on all territory on which the Kingdom has its authority, including the geographical territory of the Kingdom and its embassies in foreign jurisdictions.

Any entity, including public or private entities and natural or legal persons that process personal data inside the jurisdiction of the Kingdom is in the scope of the PDPL.

Example | Territorial scope | Processing in the Kingdom | Private entity

A hospital that is incorporated in the Kingdom processes the personal data of its employees and patients.

All of the processing takes place in the Kingdom. It includes processing of personal data of patients who come to this hospital for treatment from other countries. Therefore, the hospital must comply with the PDPL.

Example | Territorial scope | Processing in the Kingdom | Public entity

The Kingdom's Ministry of Education processes the personal data of its employees, the school-going children and teachers of the Kingdom.

All of the processing of the Ministry undertaken in the Kingdom is in scope for the PDPL.

Scenario 2: Who are considered as individuals residing in the Kingdom?

The definition of residing in the Kingdom is not limited by an individual's citizenship, his/her residence status or any other type of legal status. The PDPL applies to processing of personal data of all individuals who reside in the Kingdom, no matter their nationality or duration of residence. Such individuals include, for example:

1. citizens of the Kingdom;
2. residents of the Kingdom, including temporary and permanent workers;
3. temporary visitors of the Kingdom, including tourists and visitors (for any reasons); and
4. any other individuals who reside in the Kingdom for any reason and for any timeline, irrespective of the legal basis of the stay.

Please note that even if the individual leaves the territory of the Kingdom, his/her personal data will still be within the scope of the PDPL if such personal data is still stored in the Kingdom.

Example | Territorial scope | Residing and staying in the Kingdom as employees

A trade company operates in the Kingdom. The majority of its employees work in the Riyadh office on a permanent basis. The processing of their personal data is regulated by the PDPL.

Some of its employees are based in its Dubai office and visit the Riyadh office once a month.

When the employees from the Dubai office stay in Riyadh, the processing of their personal data is in the scope of the PDPL.

Example | Territorial scope | Visiting the Kingdom as tourists

A family from Japan visits the Kingdom as tourists. They stay in one of the hotels in Riyadh. The hotel records their personal data, including names, phone numbers, bank card numbers, and emails. After the family returns to Japan, the hotel stores their personal data for several months.

While the personal data of the Japanese family members is stored by the hotel in Riyadh, such personal data will be protected by the PDPL – even if the family no longer stays in the Kingdom.

Scenario 3: Who are considered as parties outside the Kingdom?

Any entity, including public or private entities and natural or legal persons that process personal data of individuals (who reside in the Kingdom), if processing takes place outside the jurisdiction of the Kingdom is still considered as a party of the processing. Such an entity is in scope of the PDPL and will need to comply with its obligations in respect of such processing.

Example | Territorial scope | Parties outside the Kingdom

A consulting firm based in Germany provides services to its clients based in Jeddah region. Such services include the processing of personal data of employees of the clients - for business improvement purposes.

Such processing of personal data is in the scope of the PDPL. The consulting firm is required to comply with the PDPL, even though it is not based in the Kingdom.

Example | Territorial scope | Parties outside the Kingdom

An online store operates in the Kingdom. Its customers are individuals who live and work in the Kingdom. The online store uses cloud solutions to store the personal data of its customers. The cloud solution is hosted in the USA by the US technology company.

Such storage of personal data will be regulated by the PDPL – even though the personal data is hosted in the USA.

In scenarios 1 and 2, all individuals, no matter their citizenship or residency status, are protected by the PDPL.

What roles do controllers and processors play under the PDPL?

The PDPL provides for two main roles in the data processing: a Controller and a Processor. They have different levels of responsibility in respect of the processing. The PDPL defines these terms as following.

Article 1 (18) of the PDPL

Controller: Any Public Entity, natural person or private legal person that specifies the purpose and manner of Processing Personal Data, whether the data is processed by that Controller or by the Processor.

Article 1 (19) of the PDPL

Processor: Any Public Entity, natural person or private legal person that processes Personal Data for the benefit and on behalf of the Controller.

A Controller is an entity that makes decisions about the purposes and manner of the processing. The responsibility for making such decisions can either be borne wholly by a single controller or shared among multiple controllers (e.g. if there are several Controllers in relation to the same processing activity). The Controller(s) is/are held ultimately accountable for the processing undertaken and have a larger set of obligations under the PDPL as compared to Processor(s).

A Processor is another role that is regulated by the PDPL. The Processor processes personal data on behalf of a Controller. As opposed to the Controller, the Processor does not make decisions about the purposes and manner of the processing.

Regardless of which of the two above roles you assume, the PDPL will apply to the processing of personal data by your organization in each role. Depending on the sector in which you operate, you may also need to comply with other data protection rules of the laws applicable to your sector (for example, healthcare sector, banking and financial sector).

At all times, a Controller must ensure that the Processor(s) it engages fully complies with the PDPL.

When does the PDPL not apply?

The PDPL and its provisions do not apply to you if you process personal data for family or personal purposes.

Article 2 (2) of the PDPL

The scope of applying the PDPL excludes processing of the individual›s Personal Data or purposes that do not go beyond personal or family use, as long as the individual did not publish or disclose it to others.

What is personal or family use?

Personal or family use means that an individual processes personal data within his/her family or limited social circles, which is not connected to any professional or commercial use. This does not include the publishing of personal data to a public domain or disclosing the same to anyone outside the family or personal use. This means that you are not required to comply with the PDPL if you use personal data for purely personal and family purposes. Specific types of such use depend on the context. It may include, for example:

1. communicating with relatives, friends, colleagues and other persons for personal purposes, not associated with your work;
2. taking pictures or recording videos for personal purposes; and
3. recording and sharing contact details of other individuals for personal purposes.

Example | Personal or family use | Processing outside the scope of PDPL

A group of friends celebrate a birthday in a restaurant in Dammam. During the celebrations, the friends took pictures of each other and recorded videos. Later they posted these pictures and videos on various social media networks for their own personal purposes. The pictures and videos are considered as personal data of the persons who were in these pictures and videos.

In this case, taking photos, recording videos and posting them on social media networks will not be within the scope of the PDPL.

Example | Personal or family use | Processing within the scope of PDPL

A popular blogger regularly travels all over the world and makes posts about his trips. Sometimes, he posts photos of the Kingdom's hotels and restaurants that he visits, which also contain images of others (for example, personnel of hotels and restaurants). The blogger receives payments from these hotels and restaurants for publishing such content on social media networks.

In this case, publishing photos is linked to the professional and commercial activities of the blogger. Thus, taking photos and posting them will be within the scope of the PDPL.

When will the PDPL come into force?

The PDPL came into force on 14 September 2023.

As stated in section 3 of the Royal Decree No. 19/m dated 1443/2/9, you will have a one-year grace from the effective date of the PDPL to ensure your compliance with the PDPL.

What should you do during the grace period?

During the grace period, the Competent Authority will not apply any penalties against you. However, during this period you are expected to take measures aimed at achieving compliance with the PDPL by 14 September 2024.

As stated in section 3 of the Royal Decree No. 19/m dated 1443/2/9, the Competent Authority may extend the grace period for you if your reasons for the extension are appropriate. What reasons shall be considered as appropriate will be decided by the Competent Authority in each specific case at its sole discretion.

The grace period does not relieve you from the obligation to comply with other applicable laws and regulations in the area of personal data (for example, in the financial and healthcare sector).

Who is the Competent Authority?

Pursuant to Decision of the Council of Ministers No. 98 dated 1443/2/7 SDAIA shall be the Competent Authority, for a period of two years, during which consideration shall be given – in light of the results of the application of the provisions of the PDPL and its Implementing Regulations and in light of the level of maturity in the data sector – to transferring the responsibility to supervise the application of the provisions of the Law and its Implementing Regulations to the National Data Management Office.

The key functions of the Competent Authority include, but are not limited to:

1. monitoring, investigating and enforcing compliance with the PDPL;
2. providing consultations on PDPL and other data protection legal instruments (for example, Implementing Regulations to the PDPL); and
3. management and investigation of complaints.

Individuals’ rights

The PDPL provides individuals with a number of rights. You must ensure that individuals, whose personal data you process can exercise these rights.

No.	Right of the individual	Description of the right	Articles of the PDPL
1	Right to be informed	Individuals have the right to be informed about the lawful basis for collection of their personal data, as well as of the purpose (aim) of such collection.	Art. 4 (1)
2	Right to access the personal data	Individuals have the right to access their personal data subject to meeting requirements of the PDPL and Implementing Regulations to it.	Art. 4 (2)
3	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 format.	Art. 4 (3)
4	Right to request correction	Individuals can request to have their personal data corrected (if inaccurate), completed (if incomplete) or updated (if out of date).	Art. 4 (4)
5	Right to request destruction	Individuals can request destruction of their personal data subject to requirements of the PDPL.	Art. 4 (5)
6	Right to withdraw consent	Individuals may at any time withdraw their consent which they previously gave in relation to processing of their personal data.	Art. 5 (2)

Data protection principles

Although the PDPL does not explicitly list any data protection principles, such principles are embedded in the PDPL's provisions.
Understanding these principles will help you to understand many of the requirements of the PDPL. There are seven key data protection principles that form the foundation of the PDPL. The principles are as follows:

No.	Principle	Description of the principle
1	Lawfulness, fairness and transparency	1. You must ensure that you collect personal data based on a lawful basis. 2. You must, at all times, process personal data in compliance with the laws and regulations of the Kingdom. 3. Individuals must be provided with an understanding of how their personal data is processed by you.
2	Purpose limitation	1. You need to have a specified purpose (reason) as to why you are processing the personal data. 2. You must determine the purpose of collection of personal data, which must be documented in the records of processing activities.
3	Data minimization	You must not collect more personal data than you need to achieve the purpose of processing of personal data. If you do not strictly need the personal data, you must not collect it.
4	Storage limitation	You must only process personal data for as long as you need it, unless you are obligated to store it for longer under the applicable laws (for example, specific laws of the sector in which you operate in).
5	Accuracy	1. You must regularly review personal data that you hold to ensure that it is accurate, complete and up to date. 2. You must provide an opportunity to individuals to review their personal data and update it, where necessary.
6	Integrity and confidentiality	You need to have adequate technical and organizational measures to safeguard personal data. Such controls are required to protect the confidentiality, integrity and availability of the personal data during its transmission and storage.
7	Accountability	You must have appropriate measures and records in place to be able to demonstrate your compliance with data protection laws, regulations and principles.

Please note that compliance with the above principles does not relieve you from the obligation to fully comply with all other requirements of the PDPL. However, it will serve as the foundation for effective compliance with the PDPL.

Appendix 1 - Non-exhaustive list of examples of bad data protection practices

Please see below a list of examples of bad data protection practices that violate the PDPL. The Competent Authority strongly encourages you to avoid such practices.

Please note that this list is not exhaustive and is for illustrative purposes only. Even if you avoid the practices from this list, it still means that you must comply with all the requirements of the PDPL.

Example 1 | Use of personal data without an established lawful basis

A retail electronic store collects from each customer, before completing the sale, their name, email and phone number. The customers are not provided with any explanations for such collection and are not requested to give any consent for the processing of their personal data.

After collection of the above personal data, the store:

1. places the collected personal data into a cloud storage system, hosted outside the Kingdom;
2. starts regularly sending marketing information to collected emails;
3. transfers the collected personal data to a data analytics agency.

The retail store has not identified any lawful bases for any of the above purposes of the use of personal data. The management of the store does not understand what lawful bases could be used in principle.

This is a bad practice. You must avoid it. You must always identify lawful bases for each purpose of processing of personal data, as such lawful bases are specified in Art. 5 and Art. 6 of the PDPL.

Example 2 | Collection of personal data without defined purpose

A pharmacy collects phone numbers of all its customers. When asked about the reasons for such collection, neither the cashier nor the manager of the pharmacy could explain why the pharmacy needs phone numbers. They provide an explanation such as “the pharmacy has always done so”. The pharmacy does not have any documents that show that purposes of such collection are formally defined.

This is a bad practice. You must avoid it. You must not collect personal data unless you have identified and documented purposes for such a collection.

Example 3 | Storage of personal data indefinitely

An HR department stores in its system the data about all the employees of the organization, including those who left the organization. The HR department also stores CV of all candidates that have ever applied to the organization. The personal data of all its candidates and employees is stored indefinitely and never deleted.

This is a bad practice. You must avoid it. You must destroy personal data when you no longer need it (subject to exception of Art. 18 of the PDPL).

Example 4 | Processing of personal data without a record of processing activities (RoPA)

A marketing company analyzes large volumes of personal data of various customers. The company has a number of departments with different roles.

The marketing company has not documented any of its processing activities. As a result, the management of the company does not know what types of personal data it processes, where the personal data is stored and to whom personal data is transferred.

This is a bad practice. You must avoid it. You must maintain a record of processing activities so that you understand what personal data you process.

Example 5 | Sharing of personal data without any lawful bases and without providing any privacy notice to individuals

A customer obtains a new phone number at a telecommunication company. On the same day, the company sells the database with the customer's personal data to an advertising agency. The customer was not aware of the transfer of his personal data for advertising purposes.

To his surprise, the customer starts soon receiving advertising from retail stores, restaurants, and pharmacies which he never contacted or visited.

This is a bad practice. You must avoid it. You must not share personal data with any entity, unless you have a lawful basis to do so and unless you comply with other requirements of the PDPL regarding the disclosure of personal data. The individual whose personal data you share with others must be provided with a privacy notice so that he/she understands how and why you process his/her personal data.

Example 6 | Absence of data protection-related policies and training

A pharmacy does not have any data protection-related policies or procedures in place. Further, the pharmacy's employees have not been provided training and awareness on good data protection practices. As a result, its employees do not understand how to process the personal data of its customers on a daily basis.

This is a bad practice. You must avoid it. You must have in place data protection policies and procedures that regulate how personal data is used within your organization. Once you develop such policies or procedures, it is important that they are enforced within your organization and that your employees are aware of their roles. You must regularly train your employees who handle personal data so that they do so in accordance with the PDPL and your internal policies.

Example No. 7 | Announcing patients’ personal data in the clinic

A clinic has a waiting area for its patients prior to receiving treatments. When the clinic’s doctor is ready to accept a patient, a nurse comes to the waiting area and calls out loud the patient and the reasons for the visit. All other patients in the waiting area could hear what was called out loud.

This is a bad practice. You must avoid it. The name of the patient (and the reason for the visit) is the patient’s personal data. You must ensure that the name of your client is not disclosed, other than based on the lawful bases, as specified in Art. 5, Art. 6 and subject to compliance with the additional requirements of Art. 15 PDPL.

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

National Data Governance Platform