State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

# Principles of Data Privacy

## PDPPL-02050201E

## Guidelines for Regulated Entities

**National Cyber Governance and Assurance Affairs**

**Version: 2.0**

**First Published: November 2020**

**Last Updated: September 2022**

**Classification: Public**

**Document History**

| Version Number | Description | Date |
|---|---|---|
| **1.0** | Published V1.0 document | November 2020 |
| **2.0** | Published V2.0 document | September 2022 |

**Related Documents**

| Document Reference | Document Title |
|---|---|
| **PDPPL-02050208E** | Data Privacy by Design and by Default Guidelines for Regulated Entities (English) |

# DISCLAIMER / LEGAL RIGHTS

These guidelines have been developed for controllers and processors who process personal data electronically; who collect, receive or mine personal data in anticipation of processing it electronically or who process personal data through a combination of electronic and traditional processing techniques. They also serve to provide information to individuals and other interested parties on how organisations should comply with the PDPPL.

The National Cyber Security Agency and/or the National Cyber Governance and Assurance Affairs are not liable for any damages arising from the use of or inability to use these guidelines or any material contained in them, or from any action or decision taken as a result of using them. Anyone using these guidelines may wish to consult a legal and/or professional adviser for legal or other advice in respect of these guidelines

Any reproduction of this document either in part or full and irrespective of the means of reproduction, shall acknowledge the National Cyber Governance and Assurance Affairs and National Cyber Security Agency as the source and owner of the "Controller and Processor Guidelines for Regulated Entities".

Any reproduction concerning this document for any purpose will require a written authorisation from the National Cyber Governance and Assurance Affairs and the National cyber security agency. The National Cyber Governance and Assurance Affairs and National Cyber Security Agency shall reserve the right to assess the functionality and applicability of all such reproductions of this document developed for any general intent.

The authorisation from the National Cyber Governance and Assurance Affairs and National Cyber Security Agency shall not be construed as an endorsement of the developed reproduction and the developer shall in no way publicise or misinterpret this in any form of media or personal / social discussions.

# LEGAL MANDATE(S)

Based on the Amiri Decree No. (1) for the year 2021, the National Cyber Governance and Assurance Affairs is empowered by the National Cyber Security Agency (NCSA) as the competent department for administrating and enforcing Law no (13) for the year 2016, the Personal Data Privacy Protection (PDPPL). Article 27 of the Law no (13) for the Year 2016 requires the National Cyber Governance and Assurance Affairs to take all necessary measures for the purposes of implementing the PDPPL. Article 8 of the Law no (13) for the Year 2016 requires the National Cyber Governance and Assurance Affairs to determine what 'appropriate administrative, technical and financial precautions are necessary' for Controllers to demonstrate compliance with the principles outlined by the PDPPL and protect Personal Data.

These guidelines have been prepared to take into consideration the current applicable laws of the State of Qatar. If a conflict arises between this document and the laws of Qatar, the latter shall take precedence. Any such term shall, to that extent, be omitted from this Document, and the rest of the document shall stand without affecting the remaining provisions. Amendments, in that case, shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar. The information in these guidelines is not exhaustive and should be read in conjunction with the PDPPL, guidelines issued by the National Cyber Governance and Assurance Affairs, and any related ministerial decisions.

# Table of Contents

# 1. Key points

- The purpose of this guidance is to explain the principles for the processing of personal data.
- The PDPPL sets out a number of principles for the processing of personal data. These are:
    - transparency, honesty and respect for human dignity;
    - data minimisation;
    - accuracy;
    - storage limitation;
    - integrity and confidentiality;
    - purpose limitation; and
    - accountability.
- These principles should lie at the heart of controllers' approach to processing personal data.
- The principles will guide controllers when making judgements regarding their processing, for example when deciding on the appropriate balance between the precautions for the protection of personal data against the risk of serious damage to individuals' privacy.

# 2. Introduction

The PDPPL sets out key principles for the processing of personal data. These principles should lie at the heart of controllers' approach to processing personal data and should guide controllers when interpreting the PDPPL and establishing their PDMS.

The principles should also be taken into account when putting in place appropriate precautions as determined by the National cyber governance and assurance affairs. They are particularly useful when making decisions on what level of protection is appropriate for certain personal data, and when assessing the balance between the rights of individuals and the necessity of processing their personal data.

The principles can be found in Articles 1, 3, 5 and 10 of the PDPPL, and each principle is explained in more detail below.

## Transparency, honesty and respect for human dignity

Article 3 of the PDPPL says:

> *"Each Individual has the right to the protection of the* ***Personal Data thereof that shall be processed only within the framework of transparency, honesty, and respect of human dignity****, and acceptable practices according to provisions hereof."*

This means controllers must be transparent with individuals about how they process their personal data and not process it in a misleading manner.

- Transparency is the idea that personal data must be processed in a clear, open and honest way, and in line with the right to be informed. This means informing individuals about who the controller is, and why and how the controller is processing their personal data from, who the controller is sharing it with and how long they intend to keep it;
- honesty means the personal data must be processed lawfully and not in a manner that is misleading or deceitful to the individuals concerned or for a purpose other than that which it was collected; and
- respect for human dignity relates to the right of individuals to be valued and respected, which in this context means that the use of personal data must be processed fairly and ethically.

## Data minimisation

Article 10 of the PDPPL says:

> *"The Controller shall verify that Personal Data that he collects, or being collected for the benefit thereof, is* ***relevant*** *to the Lawful Purposes and* ***adequate*** *for achieving the same...''*

The principle of data minimisation means that controllers must ensure that any personal data they process is sufficient, relevant and limited. The personal data controllers collect must be:

- adequate: the personal data they process must be adequate to fulfil their purpose;

- relevant: they must only process personal data in a way that is compatible with the original purpose for which it was processed; and
- limited to what is necessary: they must not hold more personal data than that required to fulfill the purpose for which they are processing it.

Privacy by default requires controllers to offer strong privacy defaults with respect to user preferences so that individuals should not have to take any specific action to protect their privacy. As such data should be minimised by default; i.e. an individual should not have to take any action to ensure that controllers do not collect personal data beyond the extent required or process it when not necessary.

Privacy by default is addressed in the Data Privacy by Design and by Default Guidelines.

## Accuracy

Article 10 of PDPPL says:

> *''The Controller shall also verify that such data is **accurate, complete** and **up-to-date** to meet the Legitimate Purposes.''*

Controllers must ensure personal data is correct and up to date. When processing personal data, they must:

- take reasonable steps to ensure that personal data is correct and not misleading as to a matter of fact;
- keep personal data up to date where necessary;
- take reasonable steps to delete or correct personal data that is incorrect;
- provide individuals with the means to rectify and update their personal data; and
- provide individuals with clarificatory evidence where controllers have shared inaccurate Personal Data about them.

## Storage limitation

Article 10 of the PDPPL says:

> *"The Controller shall not keep any Personal Data for a period of time that exceeds **the necessary period** for achieving such purposes."*

Controllers must not store personal data longer than is required to carry out the purpose for which they process it. When storing personal data controllers must:

- be aware of the personal data they hold and why they need to store it;
- have a policy that sets out their approach to retention periods and to erasure of personal data;
- carefully consider how long the personal data is kept and if they can justify this period; and
- regularly review the personal data they hold and erase or anonymise it when it is no longer required.

## Integrity and confidentiality

Article 3 of the PDPPL says:

> *"Each individual has a right to the **protection** of their Personal Data…"*

Article 8.3 of the PDPPL says:

> *''Take appropriate administrative, technical and financial precautions to **protect** Personal Data, in accordance with what is determined by the Competent Department.'*

Article 13 of the PDPPL says:

> *"Each of the Controller and the Processor shall take **the precautions necessary** to protect Personal Data against loss, damage, change, disclosure, access thereto, or the inadvertent or illegal use thereof."*

Controllers must ensure that they have appropriate precautions in place to protect the personal data they hold and keep it secure. The National cyber governance and assurance affairs determines that appropriate precautions to demonstrate compliance with the principle of integrity and confidentiality are to:

- ensure that controllers have processes in place to assess and implement information security measures that are proportionate to the nature and importance of the personal data being processed;
- understand which personal data controllers process will be required to be kept confidential and consider the ease with which certain personal data must be readily available.
- enable methods for encryption and/or pseudonymisation when appropriate to do so;
- maintain information security policies, procedures and technical measures and ensure that these are adhered to as well as regularly updated;
- maintain processes to test the effectiveness of controllers' measures and consider any what improvements may be necessary on a regular basis; and
- put in place technical controls such as those specified by established frameworks such as the National Information Assurance Policy 2.0.

## Purpose limitation

Article 5.3 of the PDPPL says:

> *''An Individual may at any time: Request omission or erasure of the Personal Data thereof in any of the cases referred to in the preceding two items, **upon cessation of the purpose** for which the processing has been conducted, or where **all justifications for maintaining** such Personal Data by the Controller **cease to exist**.'*

Article 10 of the PDPPL says:

> *"The Controller shall **not keep any Personal Data for a period of time that exceeds the necessary period** for achieving such purposes."*

Controllers must ensure that, by default, personal data is erased or anonymised when

they no longer need it. This means that the original purpose for which the personal data was being processed no longer exists, and there is also no longer any other legal or business justification for keeping it.

Controllers must not process personal data for purposes other than those for which it was collected unless:

- they assess that such new purpose is compatible with the original purpose; or
- they gain consent from the individual; or
- they have a legal obligation to do so.

## Accountability

Article 11.5 of the PDPPL says:

> *''The Controller **shall:** Develop internal systems for the effective management of Personal Data, and reporting any breach of measures aiming at the protection thereof;"*

Controllers must develop a Personal Data Management System (PDMS) that includes appropriate administrative, technical and financial precautions to protect personal data.

Controllers must conduct comprehensive audits and reviews on their organisation's compliance with the PDPPL, as required by Article 11.7. This is a key component to demonstrating compliance with the PDPPL.

Policies, procedures, objectives, systems and controls that are required as a part of a PDMS, should be documented, as well as records of audits and periodic reviews of the precautions controllers have in place and their effectiveness. This will help them to demonstrate their commitment to the protection of personal data and may be considered in the event of a personal data breach.

In order to demonstrate compliance with this principle controllers should implement a PDMS taking a 'privacy by design and default' approach, consisting of the precautions articulated in this PDMS guidance and any other necessary precautions that are proportionate to the nature and importance of the personal data they are processing.

## 3. Risk-based approach

Every organisation is different and there is no one-size fits-all answer to compliance with the PDPPL. It is incumbent on the controller to review and understand the requirements of the PDPPL to determine how they apply to their organisation and what they need to do to comply.

Controllers must consider the ways in which they process personal data and take responsibility for what they do with it. They must take a risk-based approach, based on the privacy principles addressed above, putting these principles at the heart of their personal data processing.

# End of Document