State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

Controller and Processor

PDPPL-02050209E

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)
PDPPL-02050205E	Individuals' Rights 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 these guidelines is to explain what a controller and processor are under the Personal Data Privacy Protection Law (PDPPL) and how controllers must comply with their obligations including the use of contracts to confirm compliance with the PDPPL of any processors that they use.
- The PDPPL places requirements on controllers and processors to protect personal data and the privacy of individuals in Qatar. An organisation is:
    - a controller with respect to a processing activity if it is the main decision-maker exercising overall control over why and how personal data is processed;
    - a processor with respect to a processing activity if it is following the instructions of a Controller or is processing personal data on their behalf; and
    - a joint controller with respect to a processing activity if it jointly makes decisions or exercises shared control over why and how the personal data is processed with another controller.
- Controllers are responsible for:
    - performing due diligence on processors to assess if they have in place the appropriate precautions to protect personal data;
    - verifying their processors' compliance with the PDPPL and their instructions and that they have appropriate precautions in place before, during and upon completion of the processing they are carrying out on their behalf. To do this they will need a written contract to formalise the relationship; and
    - informing individuals and / or the National Cyber Governance and Assurance Affairs as soon as possible after they become aware of breaches of the PDPPL or breaches of the measures they have in place to protect personal data or if any risk of threat to the personal data they are processing arises.
- Processors are responsible for:
    - their compliance with the PDPPL and adopting appropriate measures to protect personal data independently of any controller on whose behalf they are processing; and
    - informing controllers as soon as possible after they become aware of breaches of the PDPPL or breaches of the measures they have in place to protect personal data or if any risk of threat to the personal data they are processing arises.

2. Introduction

The PDPPL requires controllers to confirm that third party processors comply with the instructions they give them and adopt appropriate precautions and that such compliance must be monitored on a regular basis as part of their Personal Data Management System (PDMS). A processor is a person or organisation who processes personal data on a controller's behalf, or as per a controller's instructions.

Controllers are required to put in place measures to confirm that processors they use to process personal data comply with the requirements of the PDPPL and, in particular, that processors:

- follow through on any instructions the controller gives to them;
- establish and maintain a compliant PDMS;
- establish and maintain appropriate administrative, technical and financial precautions to protect personal data; and
- protect the rights of individuals under the PDPPL.

The definitions of a Controller and a Processor can be found in Article 1 of the PDPPL. Key requirements for Controllers and Processors can be found in Articles 8, 11 and 13 and each requirement is explained in more detail below.

2.1. How to identify a Controller or a Processor?

The PDPPL provides definitions of controllers and processors under Article 1.

Article 1 of the PDPPL says:

"...the following words and terms shall have the meanings assigned…:

Controller: **A natural** and/ or **legal person** who, whether acting individually or jointly, determines **how Personal Data** may be **processed** and determines the purpose(s) of any such processing.

Processor: A natural and/ or legal person who processes Personal Data for the Controller."

The role that the organisation plays in determining the purposes of the personal data processing dictates whether the organisation is a controller, joint-controller or a processor as set out in the key points.

3. Considerations for controllers

3.1. How do controllers determine the processors responsible for the protection of personal data?

Article 11 of the PDPPL says:

"The Controller shall:

1. **Review privacy protection measures** before proceeding with new processes; and
2. **Determine** the **Processors responsible** for protection of Personal Data..."

Controllers are required to identify their processors to comply with Article 11.2. Controllers may identify the processors they are currently engaged with through a range of means not limited to:

- reviewing their contracts to identify those that relate to services requiring the processing or transfer of personal data by or to the third-party processor;
- compiling a register of all their personal data processing, identifying processors as a part of this exercise; and/or
- developing technical data flow maps to identify personal data being transferred from their organisation to processors.

Controllers may carry out any or all of these activities to develop a complete view of the processors they use. They must determine the appropriate means of doing so and document this decision to demonstrate compliance if required by the National Cyber Governance and Assurance Affairs.

3.2. How do controllers review privacy protection measures when using a processor?

Controllers are responsible for performing due diligence on processors to assess if they have in place the appropriate precautions to protect personal data. To collect the required information from a processor they could:

- develop the DPIA with the processor, seeking their input as part of this assessment; or
- request that the processor provides information regarding their precautions for the protection of personal data to enable the controller to complete a DPIA.

This should be done when designing, changing and/or developing products, systems and services that process personal data and before proceeding with new processes as per the requirements of Articles 8.2 and 11.1 of the PDPPL.

Controllers should take the time to assess the precautions that each processor they use has in place in respect of all the personal data and processing activities they carry out on their behalf and document such assessments.

Controllers should document their decision on whether the processor has put appropriate precautions in place and include information provided by the processor. This should include an analysis of how the controller has determined that the processor's precautions are proportionate to the nature of the processing activity and whether they sufficiently mitigate any risks of serious damage to individuals.

3.3. How does a controller verify a processor's compliance with instructions and appropriate precautions?

Article 11.8 of the PDPPL says:

"The Controller shall:

Verify Processors' compliance with the **instructions** given thereto, **adoption** of **appropriate precautions** to protect Personal Data, and follow through on the same constantly."

Controllers are responsible for confirming their processors' compliance with the PDPPL and their instructions and that they have appropriate precautions in place before, during and upon completion of the processing they are carrying out on their behalf.

The appropriate administrative precaution when using a processor is to put in place legally binding responsibilities for the protection of personal data through a contract.

Following the controller's review of the processor's privacy protection measures, and prior to the processing, controllers should implement a contract between the controller and the processor setting out responsibilities for the processing and sharing of personal data.

During the processing controllers should:

- monitor the processors compliance with the contract and agreed appropriate administrative, technical and financial measures; and
- carry out any audits or reviews provided for in the contract they agreed.

After the processing, in line with the purpose limitation and storage limitation principles, controllers should:

- instruct the processor to cease processing the personal data once the purpose for processing has been fulfilled or ceases to exist; and
- confirm the processor erases such data if storage of such data is no longer necessary.

4. Considerations for Processors

4.1. What are processors' responsibilities?

The PDPPL sets out that processors are responsible for adopting appropriate precautions to protect personal data independently of any controller on whose behalf they are processing. They are also required to comply with any precautions set out in any contractual agreements they make with any controllers they are engaged with. These precautions contribute to processors' PDMS and demonstrate their compliance with the PDPPL.

Article 13 of the PDPPL says:

''The Controller and the Processor shall **adopt all necessary precautions** to protect Personal Data against loss, damage, change, disclosure and/ or illegal / inadvertent access thereto and/ or use thereof.

Precautions so adopted shall be commensurate to the nature and the importance of the Personal Data under protection.

The Processor shall forthwith **notify the Controller of any breach** of such precautions or where any risk of threats arises to Personal Data in any way."

If a processor is processing personal data on behalf of a controller, they must inform the controller as soon as possible after they become aware of one of the following events:

- they suffer a breach that results in the loss, damage, change, disclosure and/ or illegal / inadvertent access thereto and/ or use thereof;
- they find that their administrative, technical and financial measures to protect personal data have been compromised; or
- a risk of threat arises to personal data that they are processing.

This requirement enables the controller to take steps to address the breach and meet breach notification obligations under the PDPPL.

5. Contractual Considerations for Both Controllers and Processors

As set out above, controllers have a legal obligation to confirm the processor's compliance with its instructions under Article 11(8) of the PDPPL, and further to adopt appropriate precautions to protect the personal data that they process. In order for a controller to be able to carry out this legal obligation and be sure of such compliance a written contract will need to be put in place to formalise their relationship.

The purpose of this section of the guidelines is to support organisations with understanding the contractual provisions that need to be put in place, and the reasons behind these provisions.

5.1. Why is a contract important?

Aside from being a legal obligation under Article 11.8, having a written contract in place between a controller and processor is important so both parties can clearly understand their obligations and responsibilities in relation to the personal data they are processing.

The contract is also important because it ensures that:

- both parties can more easily confirm that they are complying with their obligations under the PDPPL;
- personal data of customers, employees and others is adequately protected to the standard required by the PDPPL;
- both parties understand clearly what their roles are regarding the personal data they are processing; and
- both parties can demonstrate that they are carrying out what is required of them, to both individuals and the National Cyber Governance and Assurance Affairs.

5.2. What must be included in the contract?

The contracts, both between controllers and processors and between processors and sub-processors, must set out details of the processing, specifically:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the types of personal data being processed, and the categories of individuals; and
- the controller's duties and rights.

Contracts must also include specific provisions relating to:

- the fact the processor must only process the personal data on the controller's documented instructions;
- appropriate security measures;
- the use of sub-processors;
- the duty of confidentiality;

- individuals' rights;
- the assistance that the processor must provide to the controller;
- rights regarding audits and inspections; and
- what will happen at the end of the contract.

More detail on each of these requirements is set out below.

5.3. What details of the processing must be included?

The controller must be very clear from the beginning of the working relationship as to the extent of the personal data processing it is contracting out to the processor.

The contract must include the following details about the processing:

- the subject matter, duration and nature of the processing. This means setting out for what purpose the personal data is being processed, for how long, and details on how the processing will be carried out;
- the types of personal data being processed; e.g. the categories of personal data such as names, addresses, dates of birth, etc.;
- the categories of individuals whose personal data is being processed; e.g. customers, staff, third parties etc.; and
- the duties and rights of the controller.

5.4. What must be included about the controller's instructions for processing?

The contract must state that the processor can only process the personal data on the controller's written instructions, including with regards to the transfer of personal data outside of Qatar. This is the case unless the processor is required to do so by another legal requirement.

The written instructions of the controller must:

- be documented and saved somewhere so that there is a record of the instructions; and
- make it very clear that it is the controller and not the processor that has ultimate control over what happens to and with the personal data.

If a processor acts outside of the instructions of the controller and decides itself what to do with the personal data, then the processor risks being deemed a controller itself. This could mean:

- the processor will now have to comply with the obligations of a controller under the PDPPL; and
- the processor will have the same liabilities under the PDPPL as that of a controller.

5.5. What appropriate security measures must be included?

The contract must state that the controller and processor will implement the security measures required under Article 11 and Article 13 of the PDPPL.

These security measures are as follows:

- review privacy protection measures before proceeding with new processing activities;
- set up internal complaints management systems to receive and investigate complaints, data access requests and correction requests from individuals;
- develop a Personal Data Management System (PDMS), including the ability to report any breach of data privacy measures;
- use appropriate technologies to enable individuals to exercise their rights under the PDPPL;
- conduct comprehensive audits and reviews on compliance with the data privacy requirements;
- ensure that processors comply with the instructions provided to them with regards to the processing of the personal data and ensure that processors adopt appropriate precautions to protect personal data. Such compliance and precautions must be regularly assessed by the controller; and
- take necessary precautions to protect personal data from loss, damage, modification, disclosure or being illegally or incidentally accessed or used.

Some other measures that parties may wish to oblige one another to undertake by including them in the contract include:

- encryption and pseudonymisation;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore access to personal data in the event of an incident; and
- processes for regularly testing and assessing the effectiveness of the data privacy measures.

For more information on appropriate measures, please see Data Privacy by Design and by Default Guidelines.

5.6. What must contracts say about the use of sub-processors?

Under Article 11(2) of the PDPPL, Controllers must "Determine the Processors responsible for protection of Personal Data".

As a part of compliance with this Article, the contract between the parties must include a provision governing the use of 'sub-processors'.

If a processor uses another organisation to assist in its processing of personal data for a controller, then this organisation will be a sub-processor.

The contract must include provisions to the effect that:

- the processor must obtain either a prior specific authorisation or a general written authorisation from the controller to engage any other processors (sub-processors);

- where a controller's general written authorisation is given, the processor must let the controller know of any intended changes to sub-processors, and must be given a chance to object to them;
- where a processor engages a sub-processor, it must ensure there is a contract in place which imposes the same level of data privacy obligations on the sub-processor as those included in the contract between the controller and processor; and
- the processor will be liable to the controller for the sub-processor's compliance with its data privacy obligations.

5.7. What duty of confidentiality must contracts include?

The contract must contain a provision stating that the processor will ensure that any person(s) who are processing personal data are subject to a duty of confidentiality.

This term should include the processor's employees as well as any contractors, temporary workers and third parties.

5.8. What must contracts say about individuals' rights?

The contract must contain provisions to ensure that the processor will assist the controller in responding to individuals' rights requests under Article 5 and Article 6 of the PDPPL.

These rights are as follows:

- the right to the protection and lawful processing of Personal Data;
- the right to withdraw previously given consent;
- the right to object;
- the right to erasure;
- the right to request correction;
- the right to be notified of processing;
- the right to be notified of inaccurate disclosure; and
- the right to access.

The contract should stipulate the extent to which each party is responsible for responding to Individual rights requests, which party will be responsible for the costs of such assistance and should dictate a timeline within which such assistance must be provided.

For further guidance on individuals' rights, please the Individuals' Rights Guidelines for Regulated Entities.

5.9. What assistance must be provided to the controller?

The contract must stipulate that the processor will assist the controller to ensure compliance with its obligations under the PDPPL.

These obligations include those set out in the following Articles of the PDPPL:

Article 8

- To process personal data honestly and legitimately;
- to comply with regulations enforced that concern the design, change or development of products, systems and services relevant to personal data processing;
- to take reasonable administrative, technical and financial precautions necessary to protect personal data as set out by the National Cyber Governance and Assurance Affairs; and
- to comply with relevant privacy standards, policies and guidelines established by the National Cyber Governance and Assurance Affairs.

Article 9

- Prior to processing any personal data, make the relevant individual aware of:
    - the controller's details or those of any other party conducting the processing for the controller;
    - the lawful purposes that the controller or any other party intends to achieve from the processing;
    - a full and precise description of the processing activities and the levels of disclosure of such personal data required for the lawful purposes; and
    - any other information necessary for fulfilling the conditions of personal data processing.

Article 10

- Verify that the personal data collected by the controller, or collected on its behalf, are relevant to the lawful purposes and are adequate and not excessive for achieving these purposes; and
- ensure that the personal data is accurate, complete and up to date.

Article 11

- Comply with the provisions concerning the security of the personal data processing as set out in Article 11 PDPPL. As discussed in more detail under 'Appropriate security measures' above.

Article 13

- Adopt all necessary precautions to protect the personal data against loss, damage, change, and illegal or inadvertent disclosure, access or use;
- notify the controller of any breach of these precautions; and
- notify the controller of any risk of threats to the personal data.

Article 14

- notify the NCSA/ the National Cyber Governance and Assurance Affairs and relevant individuals of any breaches of the measures to protect the individuals' privacy if such breaches are likely to cause damage to the individual.

5.10. What audit and review obligations must be included?

The contract must include obligations on the processor to assist the controller with audits and reviews of their compliance with the PDPPL, as set out in Article 11(7) of the PDPPL.

Such obligations could include:

- that the processor will allow the controller, or an auditor appointed by the controller, to audit compliance with its obligations under the PDPPL;
- that the processor will contribute to such audits where required;
- which party will be financially responsible for such audits; and,
- that the processor will make available all information as is required to show its compliance with the PDPPL to the controller. This may be via an audit, or by providing documentation of such to the controller.

5.11. What must happen to the personal data at the end of the contract?

The contract must state that at the end of the contract the processor will:

- delete or return to the controller all personal data it has been processing for the controller, and that it is the controller's choice whether such data be returned or deleted;
- delete any existing copies of the personal data, unless some other legal reason exists to keep them; and
- any deletion or return of the personal data by the processor must be done in a secure manner, in accordance with the security measurements set out in Article 11 PDPPL.

End of Document