State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

Record of Processing Activities

PDPPL-02050212E

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
N/A	N/A

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 "Record of Processing Activities 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 6

2. Introduction 7

3. What does the PDPPL say about RoPA? 8

4. How do controllers put a RoPA in place? 9

4.1. Who should put a RoPA in place? 9

4.2. What should controllers include in their RoPA? 9

4.3. What else should controllers document in their RoPA? 10

4.4. What process could controllers follow to document their RoPA? 11

1. Key points

- The Personal Data Privacy Protection Law (PDPPL) requires controllers to put in place a Personal Data Management System (PDMS).
- A key component of a PDMS is a Record of Processing Activities (RoPA) which captures key information about what personal data a Controller processes and how they do so.
- A RoPA is also an essential appropriate administrative precaution for compliance with a number of requirements of the PDPPL.
- A RoPA may also provide operational benefits for organisations such as improved data governance and management, and increased business efficiency among others.

2. Introduction

A Record of Processing Activities (RoPA) forms the backbone of a controller's data privacy compliance programme facilitating compliance with various obligations under the PDPPL.

These guidelines set out why controllers should put a RoPA in place and what this should consist of to demonstrate compliance with specific requirements of the PDPPL.

Before putting in place a RoPA, controllers should ensure they have reviewed and understood other PDPPL guidelines to enable them to capture high-quality information within their RoPA that is relevant to their processing.

3. What does the PDPPL say about RoPA?

Whilst the PDPPL does not explicitly require a RoPA, a RoPA forms the backbone of a controller's PDMS and is an appropriate administrative precaution enabling compliance with other requirements of the law. Controllers will require a RoPA to enable compliance with the requirements to:

- **track consent:** keep track of processing activities for which consent is obtained (Articles 4, 5.1, 17.2, 22);
- **publish a privacy notice:** notify individuals of information about how the controller processes individuals' personal data via a privacy notice (Articles 6.1 and 9);
- **manage privacy assessments:** keep track of Data Protection Impact Assessments (DPIAs) (Article 11.1);
- **plan training:** track personal data within their organisation to ensure staff who handle personal data are trained and aware of their responsibilities (Article 11.3);
- **manage breaches and notifications:** respond quickly and effectively to breaches involving personal data (Articles 11.5 and 13);
- **verify processors' compliance:** keep track of personal data shared with third parties (Article 11.8);
- **manage cross-border data flows:** keep track of personal data transferred to a location outside of Qatar (Article 15); and
- **manage special nature processing:** keep track of the processing of special nature personal data and manage permissions (Article 16).

As well as enabling controllers to comply with PDPPL, a RoPA can also provide other benefits such as:

- **improving data governance and management:** records of what data the controller is processing can enable good practice in data governance and management providing a consolidated view of personal data processing which can improve data quality, completeness and accuracy, and key foundations for effective data analytics, for example; and
- **increasing business efficiency:** knowing what personal data the controller holds, why they hold it and for how long it is kept may enable the development of more effective and streamlined business processes.

4. How do controllers put a RoPA in place?

The National Cyber Governance and Assurance Affairs has provided a sample RoPA template that controllers may use to document their processing activities. Controllers may use the template provided or develop their own.

4.1. Who should put a RoPA in place?

The National Cyber Governance and Assurance Affairs recommends that all controllers put a RoPA in place to keep track of their processing activities to some extent. It is ultimately for the controller to decide on whether to put a RoPA in place to support compliance with obligations under the PDPPL. If a controller does not maintain a RoPA and a complaint is made about their obligations a controller could be liable to fines under Article 23 and / or 24 of the PDPPL.

The National Cyber Governance and Assurance Affairs also recommends where a processor has a number of processing activities that they put a RoPA in place to support their compliance activities.

4.2. What should controllers include in their RoPA?

A RoPA enables controllers to meet their obligations under the PDPPL. The table below sets out information that is required to meet the obligations set out above.

Information required	Example
The name and contact details of the senior responsible staff member for privacy at the organization.	e.g. First Name, Surname, Chief Privacy Officer, email: [...], phone [...]
the name and contact details of the owner of each process;	e.g. First Name, Surname, Department, email: [...], phone [...]
the purpose of the processing;	e.g. to arrange for delivery of a product a customer orders from our company.
the permitted reason for processing;	e.g. Consent / Legitimate Interests / Legal Obligation / Contractual Obligation.
the categories of individuals whose personal data is processed;	e.g. staff, customers, students, patients, passengers, etc.
the categories of personal and/or special nature personal data processed;	e.g. ethnic origin, children, health, physical or psychological condition, religious creeds, marital relations, criminal offences and biometrics.
information regarding the DPIA for the processing activity;	e.g. a link to the completed form for the relevant DPIA or information on where it is stored.

Information required	Example
any internal parties with whom personal data is shared e.g. another department within the controller's organisation	e.g. operations department, IT department, HR department etc.
if applicable, the name or category and geographic location of any external third parties or organisations that personal data is transferred to;	e.g. [Credit Card Services Provider PLC, Doha Qatar], [Hospital Corporation Limited, London, UK], or a description such as Correspondent Banks / Travel Agents etc.
information on how long the controller retains the personal data being processed.	e.g. 1 year following initial travel date, X years in line with Central Bank requirements etc.
a general description of the controller's administrative, technical and financial precautions specifically related to security.	e.g. information regarding encryption, access controls, training etc.

**The examples provided above provide you with examples only and will not necessarily be sufficient to describe your processing activities. You are accountable for deciding what information is appropriate to enable you to comply with your obligations.*

4.3. What else should controllers document in their RoPA?

What information will be useful when drafting a privacy notice?

Controllers are required to notify individuals of certain information before processing their personal data. This is done by preparing a privacy notice to be presented to individuals prior to processing amongst other measures. The table below sets out information that controllers may wish to collect as part of their RoPA to be used when drafting their privacy notice.

Information required	Example
If consent is the permitted reason for processing, details of the specific consent statement used, the date consent was provided and information on where records of consent are stored.	e.g. Consent Statement number 123, 13th May 2017.
If legitimate interest is the permitted reason for processing, details of the legitimate interests of the processor.	e.g. a summary of the legitimate interest identified.

Information required	Example
If applicable, the existence of automated decision-making, including profiling. In certain circumstances you will need to tell people about the logic involved and the envisaged consequences of such.	e.g. a summary of how the automated decision making uses personal data to make a judgement.
If applicable, the source of the personal data. This is relevant when the controller didn't obtain personal data directly from an individual.	e.g. travel agents / price comparison websites / general practitioner upon referral.

What other information may be useful to record?

Controllers may also find it useful to record the following information:

- **contracts relating to the processing activity:** the name, owner and storage of the contract or a link to where it is held;
- **location of personal data:** the location that the personal data is stored to enable the controller to locate it easily upon an individuals' rights request or during a security breach;
- **information regarding prior breaches:** links to any documentation regarding previous breaches may enable the controller to identify any patterns or behaviours of concern;
- **additional condition for special nature processing:** the additional condition relied upon for special nature processing; and
- **permissions for special nature processing:** links to any permission obtained for special nature processing from the National Cyber Governance and Assurance Affairs that relates to the processing activity.

4.4. What process could controllers follow to document their RoPA?

As noted above, the National Cyber Governance and Assurance Affairs has provided a sample RoPA template that controllers may use to document their processing activities. They may use the template provided or develop their own.

Controllers should take a methodical approach to recording their personal data processing activities in order to be sure that they have captured the required information. The RoPA may be recorded in paper or electronic form as the controller sees fit. Controllers may wish to consider including the following steps in their initiative to develop a RoPA:

1. **confirm requirements:** Considering the measures required to develop a RoPA by confirming that they understand the requirements in the PDPPL;
2. **identify stakeholders:** Identifying key stakeholders in departments that are likely to process personal data;

3. **document format decision:** Documenting decisions on what to include in the RoPA and how this enables compliance with the PDPPL having considered these guidelines and the template provided by the National Cyber Governance and Assurance Affairs;
4. **brief stakeholders:** Making stakeholders aware of the information that they need to capture in the RoPA so that they can gather this within their departments;
5. **complete RoPA:** Ensuring that departmental stakeholders receive adequate support and guidance in completing the RoPA to ensure the information captured is enough in relation to the controllers processing activities; and
6. **ongoing review:** Reviewing the RoPA on an ongoing basis and ensuring new processing activities are added before they begin and that a member of staff is accountable for keeping it up to date and accurate.

End of Document