State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

Personal Data Management System (PDMS)

PDPPL-02050203E

Checklist 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 "Personal Data Management System (PDMS) 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. Introduction

This checklist sets out the core activities that controllers should undertake to put in place a Personal Data Management System (PDMS). Understanding whether controllers process personal data and how they do so will enable them to understand whether and how the PDPPL applies to their organisation. Personal data is information that relates to an identified or identifiable individual.

Controllers may use this checklist to plan their privacy compliance activities. This list is not exhaustive and should be read in conjunction with all guidance provided by the National Cyber Governance and Assurance Affairs as well as the PDPPL and any related ministerial decisions. Implementation of this checklist will contribute to demonstrating their compliance with the PDPPL requirement to put in place a PDMS.

This is not a self-certification checklist and completing all tasks listed does not guarantee controllers will not be found in breach of the PDPPL.

2. PDMS Checklist

All activities below are discussed in more detail in the other PDPPL guidance documents. This list provides controllers with a starting point for their privacy programme and for each tick-box section there is a corresponding guidance note. Controllers should use this list as a high-level starting point to map out their compliance activities and read the corresponding guidance as they address each area in detail.

☐ We have considered the principles of data privacy and their impact on our processing activities.

- We have reviewed the principles for the protection of personal data and understand how they form the basis for privacy. We consider these when making decisions regarding personal data at our organisation.
- These principles lie at the heart of our approach to personal data:
    - transparency, honesty and respect for human dignity;
    - data minimisation;
    - accuracy;
    - storage limitation;
    - integrity and confidentiality;
    - purpose limitation; and
    - accountability.

☐ We have considered the measures required to develop a Records of Processing Activities (RoPA).

- We have considered and documented whether we require an RoPA to enable compliance with PDPPL.
- We have identified key stakeholders in departments that are likely to process personal data.
- We have decided on a format for capturing our processing activities having considered the template provided by the National Cyber Governance and Assurance Affairs.
- We have made key stakeholders aware of the information we need to capture in the RoPA.
- We have completed our RoPA with a key stakeholder in each department and this contains the required information to support our privacy compliance programme e.g. exercise of rights, third party management, breach reporting requirements etc.
- We review our RoPA on an ongoing basis and new processing activities are added before they begin and a member of our staff is accountable for keeping it up to date and accurate.

☐ We have considered the personal data rights that individuals may invoke and are able to comply with such requests.

- We have reviewed the rights available to individuals in the PDPPL and understand what we must do to comply with the requirements. These rights are:
    - right to the protection and lawful processing of their data;
    - right to withdrawal of previously given consent;
    - right to object;
    - right to erasure;
    - right to request correction;
    - right to be notified of processing;
    - right to be notified of inaccurate disclosure; and
    - right to access.
- We have put a process in place to receive and respond to individuals' rights requests.
- We have confirmed that the relevant teams in our organisation are able to carry out the required actions to comply with each type of request following the process in place.

☐ We have a system in place to ensure individuals are able to raise concerns/ complaints.

- We have considered how to handle complaints from individuals and have a process in place to facilitate this.
- We have determined the responsible contact to handle these complaints and respond within the required time frame.

☐ We have considered the requirement to have a permitted reason for each of our personal data processing activities.

- We have determined the permitted reason for each processing activity prior to undertaking the processing, and we have documented it in our Records of Processing Activities (RoPA).
- We determine our condition for processing personal data of a special nature before we begin processing this data and document it.
- We have reviewed our Records of Processing Activities (RoPA) and identified a permitted reason for each processing activity together with our legal team.
- We have identified processes that require us to obtain individuals' consent where we do not have a lawful purpose.
- Where we are processing personal data of a special nature, we have identified both a permitted reason for the processing activity and a specific additional condition specifically for processing the special nature personal data as a condition of receiving permission from the National Cyber Governance and Assurance Affairs.
- Where a processing activity involves the processing of personal data of a special nature, we complete a DPIA due to the increased likelihood of serious damage to an individual caused by processing such data.

☐ We have considered the requirement to obtain consent where there is no alternative lawful purpose for processing or exemption.

- We have identified processes that require us to obtain individuals' consent where an applicable lawful purpose does not apply (contractual obligation, legal obligation or legitimate interests).
- We have a process in place to obtain consent, track consents provided with evidence and enable individuals to withdraw consent easily where they wish to do so.
    - our consent requires a positive opt-in and does not use pre-ticked boxes or any other method of default consent;
    - our consent statements are clear, specific and concise and separate from other terms and conditions; and
    - our consent statements name any third-party controllers who will rely on the consent.
- We ensure that we avoid making consent to processing a precondition of a service.
- We review our consents and practices for obtaining consent on an ongoing basis and, where necessary, update them.

☐ We have considered the appropriate administrative, technical and financial precautions for the protection of personal data.

- We take responsibility for complying with the PDPPL, at the highest management level and throughout our organisation and, where necessary, implement a vision, strategy and detailed governance to support our PDMS.
- We have put a process in place to build privacy into our considerations when designing new ways of processing personal data, also known as 'Data Privacy by Design'.
- We use DPIAs to assess the risk of new processing activities and determine appropriate precautions and we keep a record of these.
- Our privacy precautions are codified in an appropriate suite of policy and procedures.
- We implement appropriate security measures to protect the confidentiality, integrity and availability of personal data.
- We consider using pseudonymisation and encryption when processing personal data to reduce the risk of processing.
- We promote our employees' awareness of privacy requirements through appropriate training schemes.
- We conduct internal testing and audits of our privacy precautions on a periodic basis.
- We review our administrative, technical and financial precautions on an ongoing basis and, where necessary, update them to account for technological advances and developments in the field of privacy.

☐ We recognise the importance of conducting DPIA's in order to determine and minimise the associated risks of new processing activities.

- We have identified the processing activities we undertake that may cause serious damage to individuals (including processing personal data of a special nature) or that may require processing a large amount of personal data and we have conducted DPIAs on them.
- We have developed a process for assessing the impact of personal data processing using DPIAs and reviewing precautions to protect personal data before processing.
- Our DPIA must:
    - describe the nature and the importance of the personal data being processed under your protection;
    - identify any risk of serious damage to the individual as a result of this processing activity;
    - describe the size and scope of your operations and the financial means of your organisation;
    - consider the current state-of-the-art precautions, controls, systems, procedures and measures;
    - make an assessment of what precautions are proportionate to the nature of the processing activity and whether they sufficiently mitigate any risk of serious damage to individuals;
    - be approved by a person in your organisation who has the relevant knowledge of both the organisation and privacy; and
    - be reassessed if there is any change in the risk levels that may require further precautions to be taken.
- We ensure our staff understand the requirement to complete DPIA's before engaging in new processing activities and how to conduct them.
- We maintain a record of all DPIAs we conduct to contribute to continuous improvement and to support the rapid impact assessment required in the event of a breach.

☐ We have understood what type of personal data constitutes personal data of a special nature.

- Where we process personal data of a special nature, we identify a lawful purpose for processing *and* a separate condition for processing such data.
- We understand the categories of personal data that are of a special nature and the requirement for us to obtain permission to process such data from the National Cyber Governance and Assurance Affairs.
- We have a process in place for requesting and obtaining permission from the National Cyber Governance and Assurance Affairs.
- We monitor National Cyber Governance and Assurance Affairs publications periodically in case the minister determines additional categories of personal data of a special nature.

☐ We have understood how to identify our position either as a controller or processor which is crucial for ensuring compliance with the PDPPL.

- If we are the decision-maker exercising overall control over why and how personal data is processed, we understand our responsibilities as the controller.
- If we are following the instructions of a controller or are processing personal data on their behalf, we understand our responsibilities as the processor.
- We ensure we have appropriate precautions in place, namely written contractual requirements, to protect personal data that is being processed on our behalf by a processor.
- We have processes in place to check if processors have implemented appropriate administrative, technical and financial precautions to protect the personal data they are processing on our behalf.

☐ We have considered the implications of cross-border data transfers.

- We understand that if we collect personal data within Qatar and transfer that personal data to a location or entity that is situated outside of Qatar, this is considered a cross-border data transfer.
- We recognise when conducting cross-border data transfers that 'may cause serious damage to an individual's personal data or privacy' appropriate safeguards must be put in place to protect individuals and have a process for doing so.
- We have identified our processing activities that involve cross-border data transfers and have put appropriate safeguards in place to protect the personal data involved, unless an exception can be provided for.

☐ We have adopted precautions to protect personal data and have a plan to report breaches of such precautions.

- We understand the requirements under Article 14 of the PDPPL to notify both the National Cyber Governance and Assurance Affairs and individuals where a breach necessitates this and we have a procedure in place to do so.
- We recognise the importance of breach identification measures such as testing and scanning to ensure comprehensive information security policies.
- We understand that information security and breach response policies must be in place in order for us to include the responsibilities of our multidisciplinary team.
- We ensure processors are aware of their legal responsibility to inform us of any breaches of personal data that they are processing on our behalf.
- We maintain a record of all breaches involving personal data whether they need to be notified or not, to record our decision making and support continuous improvement.

☐ We have understood that the PDPPL has set out a number of exemptions from some of the rights and obligations in specific circumstances.

- We only process personal data under an exemption on a case-by-case basis.
- We justify and document our reasons for relying on exceptions.

- We rely on the PDPPL as normal if no exemption covers the processing activity we are carrying out.

End of Document