State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

Advisory Note on Personal Data Lifecycle Management
PDPPL-202502AN (E)

National Cyber Security Agency (NCSA)
Personal Data Privacy Protection Department (PDPPD)

Date: October 2025
Version: 1.0
Classification: Public

Document History

Version Number	Description	Date
1.0	Published V1.0 document	October 2025

Related Documents (Guidelines)

Document Reference	Document Title
PDPPL-02050201E	Principles of Data Privacy - Guideline for Regulated Entities
PDPPL-02050213E	Privacy Notice - Guideline for Regulated Entities
PDPPL-02040203E	Personal Data Management System (PDMS) - Checklist for Regulated Entities
PDPPL-02050205E	Individuals' Rights - Guideline for Regulated Entities
PDPPL-02050206E	Data Privacy Impact Assessment (DPIA) - Guideline for Regulated Entities
PDPPL-02050208E	Data Privacy by Design and by Default - Guideline for Regulated Entities
PDPPL-02050209E	Controller and Processor - Guideline for Regulated Entities
PDPPL-02050212E	Record of Processing Activities - Guideline for Regulated Entities
PDPPL-02050215E	Special Nature Processing - Guideline for Regulated Entities
PDPPL-02050217E	Personal Data Breach Notifications - Guideline for Regulated Entities

Related Documents (Assessment Tools and Templates)

Assessment Tool and Template Title
Data Privacy Impact Assessment (DPIA) - Template for Regulated Entities
Vendor Privacy Management Tool

I. DISCLAIMER / LEGAL RIGHTS

This Advisory Note has been developed for regulated entities who collect and process personal data.

The National Cyber Security Agency and/or the Personal Data Privacy Protection Department are not liable for any damages arising from the use of or inability to use this Advisory Note or any material contained in them, or from any action or decision taken as a result of using them. Anyone using this Advisory Note 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 Personal Data Privacy Protection Department and National Cyber Security Agency as the source and owner of the document.

Any reproduction concerning this document for any purpose will require a written authorisation from the Personal Data Privacy Protection Department and the National Cyber Security Agency. The Personal Data Privacy Protection Department 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 Personal Data Privacy Protection Department 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.

II. LEGAL MANDATE(S)

Based on the Amiri Decree No. (1) for the year 2021, the Personal Data Privacy Protection Department 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 Personal Data Privacy Protection Department 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 Personal Data Privacy Protection Department 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.

This Advisory Note has 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 Personal Data Privacy Protection Department, and any related ministerial decisions.

Advisory Notes complement Guidelines and are intended to extend beyond the boundaries of legal compliance. They provide practical recommendations, structured practices, and governance approaches that are essential for strengthening compliance, enhancing accountability, and embedding Data Privacy management into day-to-day operations. Guidelines and Advisory Notes form a comprehensive set of instruments in which the Guidelines anchor compliance within the law, while the Advisory Notes foster a culture of proactive risk management and accountability in improving the organizational posture on Personal Data Privacy (also referred to as 'Data Privacy').

Table of Contents

1. Introduction

The management of personal data is an ongoing process that spans multiple stages, from initial collection and processing to storage, sharing, archiving, and eventual disposal. Each stage in the personal data lifecycle presents unique challenges and compliance requirements that organizations should address to ensure the responsible handling of personal data.

This Advisory Note provides a structured framework to guide organizations in managing personal data throughout its lifecycle in compliance with the requirements of Personal Data Privacy Protection Law (PDPPL). It outlines key considerations and recommended practices for each stage, enabling organizations to establish effective controls, mitigate risks, and safeguard individuals' Data Privacy rights. The note aims to support organizations in achieving regulatory compliance while fostering a culture of accountability and transparency in personal data management.

2. What is Personal Data Lifecycle?

The personal data lifecycle refers to the series of stages that personal data goes through from its initial collection or creation to its eventual disposal. Each phase in the lifecycle presents specific responsibilities and obligations that organizations should fulfil to ensure data is handled lawfully, securely, and in alignment with regulatory requirements.

The key stages of the personal data lifecycle are tabulated below:

Lifecycle Stage	Definition
Collect/Create	The acquisition or generation of personal data for lawful purposes.
Use	Processing the personal data to meet operational, analytical, or legal requirements.
Share	Transferring personal data with appropriate safeguards within branches or offices of an organization outside of Qatar, or to third parties in or outside Qatar.
Store	Retaining data securely for a defined period, ensuring confidentiality, availability and integrity.
Archive	Moving data to non-active storage while maintaining accessibility for legal or historical purposes.
Dispose	Securely deleting or anonymizing personal data when it is no longer required.

3. Benefits of Personal Data Lifecycle Management

Proper management of personal data throughout its lifecycle is crucial for organizations to comply with regulatory requirements such as the PDPPL and to mitigate risks associated with data breaches, unauthorized access, and non-compliance penalties. The implementation of a well-defined data lifecycle management framework has many benefits, including the following:

- **Regulatory Compliance:** Ensures alignment with legal and regulatory requirements by implementing structured controls across all lifecycle stages, thereby reducing the risk of non-compliance penalties and legal actions.
- **Data Security and Data Privacy:** Protects personal data from unauthorized access, misuse, and breaches through appropriate technical and organizational measures, ensuring data confidentiality, integrity, and availability throughout its lifecycle.
- **Operational Efficiency:** Streamlines data handling processes, reducing redundancies and enhancing efficiency while facilitating quicker access to data for operational needs or compliance audits.
- **Risk Mitigation:** Identifies potential Data Privacy and security risks at each stage of the lifecycle, implements measures to mitigate them.
- **Enhancing trust and business operations:** Building trust with stakeholders by demonstrating responsible data management practices.
- **Accountability and Transparency:** Establishes clear documentation and records of processing activities, enhancing transparency with stakeholders and regulators while building trust with customers and data subjects by demonstrating responsible data management practices.

By implementing effective personal data lifecycle management, organizations can safeguard personal data, support regulatory compliance, and achieve their business objectives while ensuring Data Privacy and security.

4. Data Privacy Considerations across Personal Data Lifecycle

Managing personal data effectively requires addressing specific Data Privacy considerations at each stage of the lifecycle. Organizations should ensure that personal data is processed in a lawful, fair, and transparent manner, with appropriate safeguards applied to mitigate risks to Individuals' Data Privacy rights. The following subsections will list down the key Data Privacy considerations (in accordance with PDPPL requirements and other best practices) across the lifecycle stages; however, we recommend organizations evaluate if any other additional considerations may apply and this may depend on the nature of the underlying personal data processing activities, business operations, and regulatory landscape.

4.1. Collect/Create

- Purpose Specification: Organizations should define the specific purposes for which personal data is collected/created, ensuring it aligns with business objectives and regulatory requirements. Data collection should be justified and documented to prevent any ambiguity regarding its intended use.
- Transparency and Notice: Individuals should be provided with clear and comprehensive Data Privacy notices at the point of data collection, detailing the categories of data collected, the purpose for collection including lawful purpose, retention periods, and their rights, etc.
- Consent Management: Where applicable, explicit consent should be obtained and documented. Mechanisms should be provided to allow individuals to withdraw their consent at any time without detriment. If consent is not the appropriate lawful purpose for processing personal data, then such data collection should take place under the fulfilment of an alternative lawful purpose.
- Data Minimization: Organizations should ensure that only the minimum necessary data is collected to achieve the specified purpose.
- Accuracy: When collecting the Personal Data, Applicable Parties may need to verify the accuracy of the Personal Data being collected. Regular reviews should be conducted to verify the accuracy and relevance of collected data.
- Special Nature Data Handling: Additional safeguards should be applied when collecting personal data with special nature. Organizations should obtain PDPPD permission before processing such data and ensure compliance with applicable requirements.
- Security Measures: Adequate technical and organizational measures, such as encryption and secure transfer protocols, should be in place to protect data during collection.
- Documentation**:** Collection activities should be recorded in the Record of Processing Activities (RoPA), detailing data categories, sources, and lawful bases. The RoPA should be reviewed and updated periodically.

Reference:

Principles of Data Privacy - Guideline for Regulated Entities

Privacy Notice - Guideline for Regulated Entities

Special Nature Processing - Guideline for Regulated Entities

Personal Data Management System - Checklist for Regulated Entities

Record of Processing Activities (RoPA) - Guideline for Regulated Entities

4.2. Use

- Purpose Limitation: Personal data should only be used for the specific purposes it was collected for, as stated in the Data Privacy notice. Unauthorized repurposing or expansion of processing activities should be avoided.
- Changes to usage of personal data: If there are changes to how personal data will be used, a Data Privacy Impact Assessment (DPIA) should be conducted to evaluate potential risks. Individuals should be notified via a Data Privacy Notice, and their consent should be obtained, or a valid lawful purpose should be established before proceeding with changes to processing activities. If the use and corresponding processing activity changes involve special nature data, organizations should notify the PDPPD to validate the existing permission and ensure continued compliance with PDPPL.
- Access Controls: Personal data access should be restricted to authorized personnel on a need-to-know basis using robust access control mechanism. Regular access reviews should be conducted.
- Data Quality and Accuracy: Mechanisms should be in place to ensure that data remains accurate and up to date throughout its use. Individuals should have the opportunity to request corrections if inaccuracies are identified.
- Security Safeguards: Appropriate technical and organizational measures such as encryption, pseudonymization, awareness training and monitoring should be applied to protect data from unauthorized use, leakage, or breaches during processing.
- Audit and Monitoring: Regular audits and monitoring should be conducted to ensure data is used in compliance with applicable legal requirements and organizational policies.
- Personal Data Breach Management: The organization should establish a plan/program to manage personal data breaches. This plan/program should cover aspects from identifying a data breach to timely notification regarding the details of the data breach to relevant stakeholders including the Personal Data Privacy Protection Department and affected individuals.

Reference:

Principles of Data Privacy - Guideline for Regulated Entities

Privacy Notice - Guideline for Regulated Entities

Data Privacy Impact Assessment (DPIA) - Guideline for Regulated Entities

Data Privacy Impact Assessment (DPIA) - Template for Regulated Entities

Personal Data Management System - Checklist for Regulated Entities

Personal Data Breach Notifications - Guideline for Regulated Entities

Individuals' Rights - Guideline for Regulated Entities

4.3. Share

- Due Diligence: Before sharing personal data, organizations should assess third-party processors for their compliance with applicable Data Privacy and Data protection regulations and security standards.
- Disclosure Limitation: Organizations should limit the sharing of personal data to what is strictly necessary for the intended purpose while implementing appropriate controls to prevent unauthorized or excessive disclosure.
- Data Processing Agreements (DPAs): Legally binding agreements should be established with third parties, outlining responsibilities, security requirements, and breach notification obligations.
- Cross-Border Data Transfer Requirements: Organizations should ensure that the receiving entity provides, at a minimum, the same level of protection as required by PDPPL through contractual means.
- Periodic Assessment of Third Parties: Regularly review the Data Privacy and security landscape of Third-Party Processors to ensure ongoing compliance with PDPPL requirements.
- Changes in Data Sharing Practices: Any changes in data sharing practices should be assessed for compliance with PDPPL, with contracts and records updated to reflect the changes.
- Transparency with Individuals: Individuals should be informed about any data-sharing practices, including the purpose and recipient categories, through updated Data Privacy notices.
- Documentation: A comprehensive record of data processors should be maintained, regularly reviewed, and updated to ensure ongoing compliance.

Reference:

Controller and Processor - Guideline for Regulated Entities

Vendor Privacy Management Tool

Privacy Notice - Guideline for Regulated Entities

Record of Processing Activities (RoPA) - Guideline for Regulated Entities

4.4. Store

- Retention Period: Organizations should define retention periods for personal data in a manner that aligns with legal, regulatory, and operational requirements.

- Retention Policies: Organizations should enforce retention policies on systems and data stores to ensure personal data is retained in accordance with the defined retention periods.
- Secure Storage: Stored data should be protected using appropriate security measures such as encryption, secure access controls, and backup solutions to prevent unauthorized access, data loss, and breaches.
- Periodic Review and Cleanup: Regular reviews of stored data should be conducted to identify and remove obsolete or redundant information.
- Storage Documentation: Storage locations and methods should be documented in the Record of Processing Activities (RoPA) to ensure proper data tracking and compliance with storage policies.

Reference:

Principles of Data Privacy - Guideline for Regulated Entities

Record of Processing Activities (RoPA) - Guideline for Regulated Entities

Personal Data Management System - Checklist for Regulated Entities

4.5. Archive

- Lawful Archiving Practices: Organizations should archive data only for legitimate purposes such as compliance, audits, or historical analysis, ensuring legal justification for continued storage.
- Access Restrictions: Archived data should be subject to stringent access controls to limit unauthorized retrieval.
- Regular Reviews: Archived data should be periodically assessed to ensure ongoing relevance and compliance with retention requirements.
- Security Measures: Physical and digital security measures, such as encryption and secure storage, should be implemented to protect archived data.

Reference:

Principles of Data Privacy - Guideline for Regulated Entities

Personal Data Management System - Checklist for Regulated Entities

4.6. Dispose

- Secure Disposal Methods: Personal data that is no longer required should be securely deleted using industry-standard disposal methods to ensure irretrievability.
- Documentation and Accountability: A disposal log should be maintained, documenting what data was deleted, when, and by whom to demonstrate compliance.

- Anonymization as an Alternative: Where deletion is not feasible, anonymization techniques should be considered to prevent re-identification while preserving data value.

Reference:

Principles of Data Privacy - Guideline for Regulated Entities

Personal Data Management System - Checklist for Regulated Entities

By adopting a structured and principled approach to personal data lifecycle management, organizations can achieve compliance with PDPPL, safeguard Data Privacy, and uphold individuals' rights. This Advisory Note ensures accountability, mitigates risks, and fosters trust with stakeholders.

End of Document