State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

Advisory Note on Building a Comprehensive Data Privacy Program

PDPPL-202501AN (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-02050217E	Personal Data Breach Notifications - Guideline for Regulated Entities
PDPPL-02050215E	Special Nature Processing - Guideline for Regulated Entities

Related Documents (Assessment Tools and Templates)

Assessment Tool and Template Title
Organization Level Privacy Compliance Assessment Tool
Privacy by Design Assessment Tool
Data Privacy Impact Assessment (DPIA) - Template for Regulated Entities
Vendor Privacy Management Tool

Related Frameworks Used

Framework Title
National Incident Management Framework

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 (PDPPD) and National Cyber Security Agency (NCSA) 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

In the current digital landscape, the secure handling and management of personal data is imperative. As cyber-attacks and data breaches become increasingly prevalent, and considering the regulatory requirements set forth by Qatar's Personal Data Privacy Protection Law (PDPPL), establishing a comprehensive program for Data Privacy is of paramount importance.

2. Scope of the Advisory Note

This Advisory Note provides structured approach on how organizations can build and operationalize a Data Privacy Program from the ground up. It provides a step-by-step approach that begins with the establishment of a Data Privacy strategy and governance structure, followed by an evaluation of the organization's current Data Privacy posture, implementation of applicable Data Privacy requirements, and actions to sustain the Data Privacy Program over time.

The document is intended to support organizations in aligning their Data Privacy practices with applicable legal and regulatory obligations as well as leading Data Privacy best practices, embedding Data Privacy into business operations, and fostering a culture of accountability and transparency in personal data handling.

The Advisory Note applies to all regulated entities across various sectors that process personal data, and is intended to assist in aligning organizational practices with applicable Data Privacy and Protection obligations and best practices.

It is primarily intended for use by:

- Senior leadership, to establish oversight and accountability for Data Privacy.
- Data Privacy, legal, risk, and compliance teams, responsible for implementing and monitoring Data Privacy controls.
- Operational and supporting functions involved in personal data processing.

The Advisory Note does not prescribe a one-size-fits-all solution but provides adaptable recommendations that can be scaled according to the size, complexity, and risk profile of the organization.

The recommended approach provided in the Advisory Note is scalable and can be applied by organizations at different stages of Data Privacy maturity, whether initiating their Data Privacy journey or strengthening their existing Data Privacy Program.

3. Phases of a Data Privacy Program

A comprehensive Data Privacy Program should have the following phases:

- **Strategic Foundation (Phase I):** Laying down the fundamental frameworks and governance that drive all Data Privacy and Data Protection related activities.
- **Assess (Phase II):** Evaluating and understanding the organization's current Data Privacy landscape, compliance posture and applicable regulatory requirements.
- **Implement (Phase III):** Executing the strategies outlined in the Data Privacy program.
- **Sustain (Phase IV):** Sustaining and continuously improving the Data Privacy program.

4. Benefits of establishing a comprehensive Data Privacy Program

Following are some of the key benefits of establishing a structured and comprehensive Data Privacy Program:

- **Achieve Regulatory Compliance:** Ensure adherence to Qatar's PDPPL and other applicable Data Privacy regulations.
- **Reduce Data Privacy Risks:** Identify, assess, and mitigate risks associated with data processing and potential breaches.
- **Enhance Stakeholder Trust:** Demonstrate accountability and transparency in handling personal data.
- **Improve Operational Effectiveness:** Integrate Data Privacy practices into business processes to optimize personal data management.
- **Foster a Data Privacy-Aware Culture:** Promote awareness and responsibility across all levels of the organization.
- **Reduction of costs:** Reduce long-term operational costs and lower the risk of fines due to non-compliance of regulatory requirements.

5. Phase I: Strategic Foundation

This phase focuses on laying down the fundamental frameworks and principles that drive all Data Privacy and Data Protection related activities. It involves creating a Data Privacy program charter, establishing a Data Privacy Office, and setting the strategic direction for Data Privacy efforts within the organization.

5.1. Design a Data Privacy Program Charter, Vision, and Mission

Creating a Data Privacy program charter along with a clear vision and mission for Data Privacy practices establishes a strong foundation and clear direction for the organization's Data Privacy efforts. This charter should outline the Data Privacy program's scope, objectives, and key responsibilities, aligning with the organizational goals and Data Privacy compliance requirements. The vision and mission statements should articulate the long-term goals of the Data Privacy program, emphasizing the organization's commitment to protecting personal data and upholding Data Privacy as a core value.

Reference: '*Privacy Governance*' domain of '***Organization Level Privacy Compliance Assessment Tool***'.

5.2. Data Privacy Governance Structure

A Data Privacy Governance Structure ensures that Data Privacy management is embedded within the organization and there is accountability with clearly defined roles and responsibilities assigned to appropriate departments for ensuring Data Privacy compliance. The establishment of a Data Privacy Office serves as the hub for Data Privacy-related initiatives, responsible for developing, implementing, and overseeing the organization's compliance to PDPPL and other applicable requirements. The Data Privacy Office can be a department of its own with a dedicated Data Privacy Officer or can be a role within another appropriate department (generally this would be a role in the Legal Department). The DPO role should be in a position to perform their duties and tasks in an independent manner, and its core activities should relate to overseeing and implementing primary activities, rather than ancillary acts which should be carried out by different functions depending on the organization's structure, Data Privacy risk exposure and business priorities. Some examples of responsibility structure are listed below along with the benefits and challenges:

- Information Security Office: Aligns Data Privacy with cybersecurity measures but may focus more on security risks than broader Data Privacy compliance.

- Data Management Office: Integrates Data Privacy into data governance strategies but may prioritize data utilization over regulatory compliance.
- Legal/Compliance: Strengthens regulatory adherence and risk management, but may lack direct operational control over cybersecurity and data functions.

To operationalize Data Privacy, Data Privacy Champions are recommended to be appointed within departments to ensure that Data Privacy is embedded in daily operations. These champions serve as the liaisons between the Data Privacy Office and departments, helping to drive compliance and awareness.

6. Phase II: Assess

In this phase, the organization evaluates and understands its current Data Privacy landscape, applicable requirements and compliance posture. This includes identifying personal data being processed, conducting a current state Data Privacy compliance assessment, and developing a roadmap to address any identified compliance gaps.

6.1. Personal data Inventorization

The first step in the assess phase is to identify what personal data is being processed within the organization. This begins with creating a comprehensive inventory or records of processing activities (please refer to the section 4.3 of the RoPA Guideline for developing RoPAs).

This activity should be performed at a Business Unit/ Process level to ensure completeness across the entire organization. This is essential for gaining insight into the flow of data across the organization. It entails categorizing the various types of data being processed, understanding the purposes for which the data is processed, and documenting the flow of this data through the organization's systems and processes. This meticulous approach is critical for identifying potential Data Privacy risks and establishing clear accountability measures.

Further, the RoPAs developed should be periodically reviewed to check if there are any updates to underlying processing activities and also ensure all new processes are documented in the RoPA.

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

6.2. Data Privacy Compliance Assessment and Roadmap Development

Performing a current state assessment is crucial for identifying the applicable requirements and assessing any gaps as well as the risk level status of non-

compliance. This assessment should be spearheaded by the Data Privacy Office, with ample support provided by other business units.

Following the assessment, an actionable implementation roadmap should be developed by the Data Privacy Office with support from other relevant stakeholders to address any non-compliances that may have been identified during the assessment activity. This roadmap should include the necessary compliance initiatives and action items to address the non-compliances along with the associated timelines and responsible stakeholders. Data Privacy Office should use this roadmap to track the progress with regards to PDPPL compliance initiatives.

Reference: ***Organization Level Data Privacy Compliance Assessment Tool***

7. Phase III: Implement

This phase involves executing the strategies outlined in the Data Privacy program. Key activities include developing and refining Data Privacy policies and procedures, managing the personal data lifecycle, providing Data Privacy notices to individuals, managing third-party Data Privacy risks, handling individual rights requests, special nature processing and implementing measures for personal data breach management and Data Privacy by Design.

7.1. Development of Policies and Procedures

The results of the Current State Compliance Assessment and the Implementation Roadmap should guide the development and refinement of Data Privacy policies and procedures. Establishing comprehensive Data Privacy policies and procedures is critical to ensuring compliance with the Personal Data Privacy Protection Law (PDPPL). It is recommended to develop an overarching Internal Data Privacy Policy that addresses all the applicable Data Privacy requirements within the organization and develop dedicated policies and procedures with additional emphasis on PDPPL compliance requirements such as the management of individual rights, data breaches, data retention and disposal, oversight of data processors, etc.

The Data Privacy Office should ensure all Data Privacy related policies and procedures are periodically reviewed and formally approved by the Top Management, reinforcing organizational commitment and accountability for Data Privacy compliance. They should also actively communicate these policies and procedures to all employees, monitoring relevant departments to ensure that employees are appropriately trained within their respective departments and are well informed and have easy access to the necessary resources.

Reference: ***Personal Data Management System - Checklist for Regulated Entities***

7.2. Personal Data Lifecycle Management

Implementing personal data lifecycle management in accordance with the Personal Data Privacy Protection Law (PDPPL) involves a structured approach from data collection to disposal, ensuring adherence to PDPPL requirements and safeguarding individuals' Data Privacy. Organizations should start with meticulous data collection, gathering only essential information with appropriate consent (if applicable) or for another lawful purpose. Processing Personal Data should be done in a secure manner where access of Personal Data should be limited to authorized personnel and to those persons who are required to have access to such Personal Data to fulfil the purpose. Where appropriate, organizations should implement encryption and perform regular audits to test for integrity and confidentiality. Employees or persons involved during Processing of the Personal Data should have appropriate training, including the secure sharing the Personal Data to a third party and actions to be taken and notifications in the event of a breach. Finally, it is imperative to establish clear procedures for the disposal of personal data, in line with the organization's data retention policies and legal requirements.

Reference: ***Principles of Data Privacy - Guideline for Regulated Entities***

7.3. Data Privacy Notice to Individuals

Providing clear, concise, and accessible Data Privacy notices to individuals about the processing of their personal data is a requirement under the PDPPL. Data Privacy Notices should be provided for in writing, including, where appropriate by electronic means Organizations are required to identify the various categories of individuals whose personal data is being processed and ensure they provide these individuals with a Data Privacy Notice at the time of data collection. The Data Privacy Notice should cover the following with regards to how their personal data is being processed:

- Identity and contact details of the Controller
- The contact details of the Data Privacy Office/Officer, where one is appointed or where there is a dedicated department
- What personal data is processed highlighting where such data is of a special nature
- How personal data is collected
- Permitted Reasons for collecting and processing personal data
- Permitted Reasons for disclosing personal data to other parties
- The length of time personal data is retained for
- Description on how personal data is kept secure

- Various rights that are available for individuals to exercise under PDPPL
- Individuals right to file a complaint to the PDPPD for PDPPL
- Details of any cross-border data disclosures
- Details of any automated decision-making including profiling.

Further, if consent is identified as the lawful purpose for processing personal data, explicit consent should be obtained from the individuals by presenting the Data Privacy Notice.

Reference: ***Privacy Notice - Guideline for Regulated Entities***

7.4. Third Party and Cross Border Data Privacy Risk Management

Third parties that process data on behalf of the organization present unique challenges and risks. Third Party Data Privacy Risk Management process starts with identifying all the Data Processors that are currently being used and this is to be followed up with execution of Data Processing Agreements which should include appropriate Data Privacy and Data Protection clauses. It is also advisable to subject these Third-Party Processors to periodic audits. Further, it is also required to ensure that appropriate due diligence is conducted prior to onboarding a prospective Third Party as a Data Processor.

In some scenarios, the Third Party can be another controller and, in such instances, a joint controller agreement should be established and executed to clearly identify each parties' responsibilities and limitations with regards to personal data processing.

For managing risks arising from cross border data transfers, the organization should perform the following:

- Identify and record all cross-border data transfers of personal data
- Perform a risk assessment to identify and manage any risks that may arise from such data transfers
- Ensure the data importing entity established outside Qatar processes personal data in accordance with PDPPL requirements and this shall be ensured via appropriate contractual measures.

Reference:
Controller and Processor - Guideline for Regulated Entities

Privacy Management Tool

7.5. Individual Rights Management Program

A program that efficiently handles individuals' rights is essential under the PDPPL. This program should notify individuals on the existence of their Data Privacy rights and allow individuals to exercise the following rights in a timely manner:

- Right to be notified of processing
- Right to access
- Right to request correction
- Right to erasure
- Right to withdraw consent
- Right to object
- Right to be notified on inaccurate disclosure
- Right to protection and lawful processing.

Upon receiving a request from an individual to exercise his/her rights, the organization should respond to the individual that they will respond to the right request and in a timely manner. Further, the organization should also verify the identity of the individual prior to fulfilling the individuals rights request to prevent malicious individuals from exercising the rights of other individuals. In cases where organizations have a valid reason to not fulfil an individual rights request, they should notify such individuals with the reasons behind doing so.

Reference: ***Individuals' Rights - Guideline for Regulated Entities***

7.6. Personal Data Breach Management

Data Privacy incidents and personal data breaches involve unauthorized access, disclosure, loss, or alteration of personal data. To manage these effectively, organizations should establish a cybersecurity incident response process aligned with the National Information Security Incident Management Framework (NIMF), while complying with Article 14 of the Personal Data Privacy Protection Law (PDPPL), which requires notifying the PDPPD and affected individuals within 72 hours if the breach is likely to result in serious harm.

- **Notification & Categorisation:** Employees should promptly report any suspected Data Privacy incident to the Data Privacy and Information Security teams. An initial assessment should be conducted to understand the nature and scope of the breach. If serious harm is likely, the PDPPD and affected individuals should be notified within 72 hours. For incidents involving national-level cybersecurity impact, the NCSA should be notified within 2 hours.
- **Initiation:** A cross-functional response team should be activated, including members from Data Privacy, Information Security, Legal,

HR, and Communications. The team should begin documenting the incident, initiate containment actions, and preserve relevant evidence while coordinating the next steps.

- **Response and Investigation:** The team should determine what personal data was involved, how the breach occurred, and assess the overall impact. A root cause analysis should be carried out, and forensic data collected if needed. Communication should be maintained with internal and external stakeholders, and coordination with Sectoral CERTs or the NCSA should be initiated if applicable.
- **Remediation & Recovery:** Appropriate corrective actions should be implemented to prevent recurrence, including technical fixes, access restrictions, or policy changes. Affected individuals should receive further guidance if ongoing risks are identified.
- **Closure & Review:** A formal review should be conducted after resolving the breach to identify lessons learned and improve future response efforts. The breach should be documented in the organization's register, and internal procedures should be updated to reflect any identified gaps.

Reference:
Personal Data Breach Notifications - Guideline for Regulated Entities

National Incident Management Framework

7.7. Data Privacy by Design

A comprehensive approach to Data Privacy by Design is essential for embedding Data Privacy considerations into new projects, products, and business processes from the outset. This methodology helps to minimize Data Privacy risks and can lead to more innovative and Data Privacy-friendly solutions. The following are key steps for effectively implementing Data Privacy by Design:

- **Data Privacy Impact Assessments (DPIA):** Subject all proposed processes and projects to a DPIA to identify and mitigate Data Privacy risks. This assessment should be conducted before proceeding with any new initiative to ensure compliance with Data Privacy regulations and protect individual rights.
- **Privacy by Design Assessment:** Ensure proposed products undergo a Privacy by Design Assessment using the tool published by PDPPD. This assessment evaluates the product's design to confirm that Data Privacy principles are embedded from the start, including

considerations such as data minimization, user consent, transparency, and security.

- **Incorporate Data Privacy into Design and Processes:** Ensure that Data Privacy is a fundamental component of both system architecture and business processes. Implement technical and organizational measures that protect Data Privacy by default across all aspects of the organization.
- **Employee Training and Awareness:** Train employees on the principles of Data Privacy by Design and their role in maintaining Data Privacy standards. Conduct regular awareness programs to keep staff updated on best practices and regulatory changes.
- **Regular Reviews and Updates:** Continuously review and update Data Privacy policies, procedures, and practices to adapt to new threats, technological advancements, and regulatory changes. Regular audits and assessments help identify areas for improvement and ensure ongoing compliance.

Reference:

Data Privacy by Design and by Default - Guideline for Regulated Entities

Privacy by Design Assessment Tool

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

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

7.8. Special Nature Processing

A comprehensive approach to managing the processing of personal data with a special nature is essential for ensuring compliance with PDPPL requirements and protecting individual Data Privacy. The following are key steps for effectively managing special nature processing:

- **Identify Special Nature Data:** Identify all processing activities which involve processing personal data with a special nature.
- **Obtain Permission:** For the identified special nature data processing activities, obtain permission from the PDPPD. This includes:
  - **Conducting a Data Privacy Impact Assessment (DPIA):** Identify the risks of processing and actions to mitigate those risks.
  - **Identifying Permitted Reasons and Conditions:** Document both a permitted reason for processing and an additional condition for special nature processing in their records.

- **Submitting a Request:** Submit a request for permission to process special nature personal data to the PDPPD.

- **Enhanced Security Measures:** Implement stronger security controls, such as encryption, access controls, and anonymization, to protect personal data of a special nature from unauthorized access and breaches.

- **Monitor and Review:** Regularly monitor and review special nature data processing activities to ensure ongoing compliance with Data Privacy laws and address any emerging risks.

Reference: ***Special Nature Processing - Guideline for Regulated Entities***

8. Phase IV: Sustain

The final phase focuses on sustaining and continuously improving the Data Privacy program. This involves continuous monitoring and improvement of Data Privacy practices, and maintaining an effective employee training program to ensure all staff understand their roles in maintaining Data Privacy and compliance.

8.1. Continuous Monitoring and Improvement

Continuous monitoring and improvement are imperative for sustaining compliance and for adapting to changes in business or regulatory landscape. Organizations should:

- **Regularly Review Data Privacy Practices:** Conduct periodic assessments of Data Privacy practices to identify areas for enhancement and ensure ongoing compliance with regulatory requirements.

- **Stay Abreast of Legislative Developments:** Keep updated with changes in Data Privacy laws and regulations to ensure the organization's practices remain compliant.

- **Conduct Audits and Assessments:** Perform regular internal and external audits to evaluate the effectiveness of Data Privacy controls and identify any gaps or weaknesses.

- **Periodic DPIAs and update RoPAs:** Depending on the type of Personal Data being processed, the extent of the Processing and whether there have been any changes to the Processing, DPIAs should be carried out and RoPAs to be updated on a periodic basis to assess

changes in risk exposure and document changes to the personal data processing landscape.

- **Integrate Feedback:** Collect and integrate feedback from various stakeholders, including employees, customers, and regulators, to refine and improve the Data Privacy program.

8.2. Employee Training Program

An effective employee training program is key to ensuring that all staff members understand their role in maintaining Data Privacy and compliance. The training program should:

- **Cover Key Elements of the PDPPL:** Ensure employees are well-versed in the main provisions of the PDPPL and understand their responsibilities under the law.
- **Organization-Specific Data Privacy Practices:** Educate employees about the organization's specific Data Privacy policies, procedures, and best practices.
- **Responding to Individual Requests:** Train employees on how to handle individual requests regarding their data, including access, correction, and deletion requests.
- **Handling Data Breaches:** Equip employees with the knowledge to identify and respond to potential data breaches, ensuring timely and appropriate actions are taken.
- **Regular Updates and Refreshers:** Conduct regular training sessions and refresher courses to keep employees updated on the latest Data Privacy practices.

Implementing a robust Data Privacy compliance program is critical for compliance with the PDPPL and for the overall protection of personal data within the organization. By following the structured approach outlined in this Advisory Note, organizations can systematically enhance their Data Privacy practices. This not only ensures legal compliance but also builds trust with individuals and stakeholders. Continuous improvement and regular employee training are essential to adapt to evolving Data Privacy challenges. Ultimately, a well-established Data Privacy program fosters a culture of Data Privacy and Data Protection as core organizational values.

End of Document