State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

Data Privacy Impact Assessment (DPIA)

PDPPL-02050206E

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-02050203E	Personal Data Management System (PDMS) Checklist for Regulated Entities (English)
PDPPL-02050208E	Data Privacy by Design and by Default Guidelines for Regulated Entities (English)
PDPPL-02050204E	Permitted Reasons Guidelines for Regulated Entities (English)
PDPPL-02050201E	Principles of Data Privacy Guidelines for Regulated Entities (English)
PDPPL-02050502E	Data Privacy Impact Assessment (DPIA) Template 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 "Data Privacy Impact Assessment (DPIA) 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 DPIAs? 8
4. What is a DPIA? 9
   4.1. What does a DPIA include? 9
   4.2. What are the key outcomes of a DPIA? 9
5. When should controllers perform a DPIA? 11
   5.1. What does "may cause serious damage" mean? 11
   5.2. How may a DPIA be helpful in the event of a breach? 12
   5.3. How do I assess whether a processing activity "may cause serious damage?" 12
6. How do controllers conduct a DPIA? 14
   6.1. Who should be involved in completing a DPIA? 14
7. What are the steps to completing a DPIA? 15
   7.1. Provide details of process ownership 15
   7.2. Document a decision on whether to carry out a DPIA or not 15
   7.3. Provide details of the processing activity 15
   7.4. Assess necessity and proportionality 16
   7.5. Conduct risk assessment and identify risk mitigating actions 16
   7.6. Assess the potential for serious damage against measures identified 16
   7.7. Assess how the controller will demonstrate adherence to PDPPL principles 17
   7.8. Sign off 17
   7.9. Actions following DPIA 17
8. Appendix A - Example DPIA Triggers 18

1. Key Points

- The purpose of these guidelines is to explain the requirement for controllers to conduct Data Privacy Impact Assessments (DPIA) prior to processing personal data under Article 11.1 of the PDPPL.
- A DPIA is an assessment to identify the risk of processing personal data to individuals and mitigate the risk of processing to an acceptable level.
- It is a key component of a Personal Data Management System (PDMS) and helps demonstrate Data Privacy by Design and Default.
- Controllers must implement a process to manage DPIAs and provide training to their people on how to conduct them.
- Controllers should perform a DPIA prior to processing personal data in a new way or prior to making a significant change to a current processing activity. They should embed any risk mitigation actions identified into the project plan for the initiative to ensure they are carried out.
- Under the PDPPL controllers are accountable for how they process personal data and for minimising the risk to individuals and their data. Keeping a record of DPIAs is an important way to demonstrate compliance.

2. Introduction

The PDPPL requires controllers to undertake an assessment of proposed privacy protection measures prior to proceeding with new processing. This assessment is known as a Data Privacy Impact Assessment (DPIA). Processing personal data poses risks to individuals and their personal data. Conducting a DPIA enables controllers to identify these risks and implement a plan to mitigate them. DPIAs are a key component of a Personal Data Management System (PDMS). For more information on PDMS, please see the Personal Data Management System (PDMS) Checklist for Regulated Entities.

The requirement to assess the proposed privacy protection measures prior to processing can be found in Article 11 of the PDPPL and the requirements to implement appropriate measures to mitigate the risks of processing can be found in Article 13.

3. What does the PDPPL say about DPIAs?

Article 11.1 of the PDPPL says:

> ''The Controller shall take the following procedures: 1. Reviewing privacy protection measures before proceeding with new processing operations.''.

Article 13 of the PDPPL says:

> "Each of the Controller and the Processor shall take the precautions necessary to protect Personal Data... Such precautions shall be commensurate with the nature and the importance of the Personal Data intended to be protected."

Prior to processing personal data, controllers must:

- identify the risk posed to individuals by the proposed processing activity;
- review the proposed precautions to protect personal data privacy; and
- assess the potential impact on individuals of any new processing activity.

Controllers must put in place administrative, technical and financial measures to keep personal data secure, private and processed in compliance with the principles of the PDPPL that are commensurate to the nature and importance of the personal data being processed and the associated risks.

Conducting an effective DPIA demonstrates compliance with the PDPPL, providing a record that controllers have conducted the required review under Article 11.1 and have identified appropriate precautions to be put in place under Article 8(3) and 13.

4. What is a DPIA?

A DPIA is an assessment to identify the risk of processing personal data to individuals and mitigate the risk of processing to an acceptable level. It is similar to a risk assessment and should be performed consistently in a standardised manner across the organisation.

4.1. What does a DPIA include?

A DPIA:

- establishes the details of a processing activity including:
    - what personal data is processed;
    - why the personal data is processed;
    - how the personal data is processed; and
    - who within an organisation is responsible.
- Identifies the risks of processing to individuals and of potential non-compliance on the organisation;
- identifies potential mitigants to those risks;
    - articulates a decision on what mitigating actions are proportionate to the risks posed and a justification for any actions that are identified but not taken;
    - identifies the need to consult with the National Cyber Governance and Assurance Affairs if risks cannot be appropriately mitigated; and
    - captures approval from the appropriate responsible person(s) of the assessment and plan to implement mitigating actions identified.

4.2. What are the key outcomes of a DPIA?

The key outcomes of a DPIA:

- Controllers have an actionable risk treatment plan consisting of measures to reduce the risk of serious damage that the processing activity may cause to an appropriate level. Such precautions are not mutually exclusive and could be:
    - Administrative: for example, a new or updated policy, process, training, governance and/or segregation of duties.
    - Technical: for example, encryption, anonymisation, pseudonymisation and/or access controls.
    - Financial: for example, investment in a service and/or technology.
- Controllers have a reasoned assessment documented as evidence that appropriate measures have been identified to protect the personal data to be processed and can justify their assessment that such measures sufficiently minimise the risk of serious damage.
- Controllers can quickly assess the potential for serious damage in the event of a personal data breach because they have a record of their DPIA.

- Controllers have a record of their decision-making to demonstrate compliance with Articles 11 and 13 in line with the principle of accountability.
- Controllers have the information required to consult the National Cyber Governance and Assurance Affairs if they cannot sufficiently mitigate the risk of processing.

5. When should controllers perform a DPIA?

Controllers should carry out a DPIA before beginning any new activity that involves processing personal data or before making significant changes to an existing activity. It is good practice to review DPIAs periodically to check that they are up to date.

DPIAs are particularly important when carrying out a processing activity that "may cause serious damage" to the individuals whose personal data controllers are processing. This means that although they have not yet assessed the level of risk in detail, controllers need to screen for factors that point to the potential for a widespread or serious impact on individuals.

Examples of activities that may trigger a DPIA are:

- technology implementations or upgrades;
- changes to existing processes; and
- changes to products or services.

More examples are provided in the appendix.

Controllers must decide whether a DPIA is required in line with the principle of accountability. If they do not undertake a DPIA where clearly required to do so, they could be liable for a fine of QAR1,000,000 under Article 23 of the PDPPL.

A DPIA can cover a single processing operation, or a group of similar processing operations. Controllers may even be able to rely on an existing DPIA if it covered a similar processing operation with similar risks. They are accountable for justifying how similar the processing activities are and whether relying on an existing DPIA is appropriate. They should document this justification.

Where controllers are using a third-party processor, they may be able to use a DPIA that they have carried out to inform their own DPIA. An example of this would be a Controller engaging a service provider to provide a direct mailing application requests a copy of the DPIA that the provider conducted when developing the application to provide information on risks and potential mitigating actions that the Controller could put in place.

5.1. What does "may cause serious damage" mean?

The PDPPL does not define what "may cause serious damage" means. Before processing personal data controllers should assess whether serious damage could be caused to the individual's privacy or personal data. The PDPPL explicitly states two specific ways of processing that may cause serious damage. These are:

- transferring personal data outside the State of Qatar, known as a cross-border data transfer; and
- processing personal data of a special nature, specific categories of personal data also known as sensitive personal data.

Controllers should consider the potential impact on individuals and damage your processing may cause – whether physical, emotional or material. In particular, examples of risks of damage could be where the processing could contribute to:

- inability to exercise rights;
- inability to access services or opportunities;
- loss of control over the use of personal data;

- discrimination;
- identity theft or fraud;
- financial loss;
- reputational damage;
- physical harm;
- loss of confidentiality;
- re-identification of pseudonymised data; or
- any other significant economic or social disadvantage.

Serious damage is not limited to the damage caused in the event of a breach. It could be related to unfairly processing personal data which could result in decisions being taken about individuals which are not in line with the principles of processing or adversely impact their rights.

5.2. How may a DPIA be helpful in the event of a breach?

The PDPPL also requires controllers to notify the Individual and the National Cyber Governance and Assurance Affairs of any breach that "may cause serious damage" to an individual's privacy or personal data. Such a breach could be a breach of security, for example, the theft of personal data but it could also be a breach of the principles, for example, not processing personal data transparently by not providing an adequate privacy notice.

In the event of a personal data breach, a Controller's database of DPIAs will enable them to establish whether the breach is likely to have caused serious damage to individuals and inform their breach response decision-making, including whether notifications are required. As such, DPIAs are an essential part of Controllers' personal data breach preparedness.

5.3. How do I assess whether a processing activity "may cause serious damage?"

A DPIA should be performed for any new processing activity. For existing processing activities, it is good practice to undertake a DPIA to assess any significant risks the processing may pose to individuals' privacy or personal data that require mitigation. Controllers must carry out a DPIA for any processing activity that "may cause serious damage."

In order to decide whether a DPIA is necessary, controllers should make a high-level judgement to identify whether there are characteristics that indicate potential for serious damage. Controllers should screen for any indications that they need to do a DPIA to look at the risk (including the likelihood and severity of potential damage) in more detail.

To decide whether their processing "may cause serious damage" and will require a DPIA, controllers should consider if their processing activity involves one or more of the following:

- processing any special nature personal data;
- using a new innovative technology or an existing technology in a new way;
- carrying out automated decision-making which leads to a decision to limit an individual's access to a product, service, opportunity or benefit i.e. decisions made by a computer without human involvement;
- collecting personal data via third parties instead of directly from individuals;

- tracking individuals or monitoring their behaviour (e.g. CCTV, online browsing patterns, GPS location tracking);
- undertaking a cross-border personal data transfer i.e. transferring personal data outside of the State of Qatar;
- processing employees' personal data;
- using personal data to target direct marketing at individuals;
- marketing or provision of goods or services to children (eg sending promotional emails to children) without parental consent; and
- carrying out a processing activity that is new to their industry.

As a matter of good practice, a DPIA should be continuously reviewed and regularly re-assessed. Therefore, we would expect controllers to decide to conduct DPIAs on their existing processing activities, based on the criteria above, as part of their obligations in line with the principle of accountability.

Ultimately, it's up to controllers to decide whether their processing may cause serious damage to individuals, taking into account the personal data processed and the nature of the processing. If in any doubt, they should conduct a DPIA to ensure compliance and demonstrate best practice.

For activities that may not cause "serious damage," Controllers must document evidence that they have considered the need for a DPIA. A record of this decision serves as evidence that privacy risks are considered before implementing a processing activity in line with data privacy by design and default. For more information please see the Data Privacy by Design and by Default Guidelines.

6. How do controllers conduct a DPIA?

At a high level, a DPIA must:

- describe the nature and the importance of the personal data that is necessary for this processing activity, including but not limited to amount and sensitivity;
- identify the risks of serious damage to the individual;
- describe the size and scope of the Controller's operations and the financial means of their organisation;
- assess whether the purpose of processing can be achieved using any other means that involves processing of less personal data;
- consider the current state-of-the-art functions, processes, controls, systems, procedures and other measures for protecting personal data; and
- make a judgement on what measures to protect the personal data are proportionate to nature of the processing activity and the risks of serious damage to individuals and sufficiently mitigate the risks involved.

A DPIA should be documented in clear and concise language with a non-specialist audience in mind, explaining any technical terms and acronyms that are used.

We have provided a sample DPIA form that controllers may use to conduct their DPIAs. They may use the template provided or develop their own. A DPIA is supposed to be flexible and scalable if:

- controllers are a small organisation with relatively simple processing activities, their DPIAs will likely not be overly detailed; and/or
- controllers are a multinational company processing personal data in a complex way with cutting edge technology, controllers will likely need to consider the impact of such processing in depth to be able to confirm that their privacy protection measures are proportionate to the risk of serious damage.

6.1. Who should be involved in completing a DPIA?

The DPIA should be completed by a person or group of people that bring together:

- sufficient detailed knowledge of the proposed processing activity, often this will be provided by the process owner;
- sufficient understanding of PDPPL requirements and data protection concepts and practices, often this will be provided by a data protection officer or champion; and
- sufficient authority to sign off the judgement made as to whether the appropriate precautions are proportionate to the nature of the processing activity.

7. What are the steps to completing a DPIA?

The DPIA Form is often completed by the process or project owner or project team in consultation with a colleague trained in data protection.

They should consult with all relevant stakeholders, both internally and at any third parties, to ensure they capture all relevant risks arising from the processing activity, in particular those that may cause serious damage.

It should be approved by someone with appropriate authority to do so and someone with sufficient data protection knowledge, for example, the head of the department that owns the processing activity and the head of data protection.

We have set out the areas that a DPIA should cover below with guidance on what information should be provided. These guidelines align to the fields within our sample DPIA form and should be read in conjunction with it.

7.1. Provide details of process ownership

Controllers should identify who will own this processing activity within their organisation. It should be the single employee, role, department or team who is in charge of the day-to-day decisions required to operate the process.

These individuals or teams are responsible for the processing, but controllers are ultimately accountable for it and for the protection of personal data processed.

Please refer to section (a) of the Data Privacy Impact Assessment (DPIA) Template for Regulated Entities.

7.2. Document a decision on whether to carry out a DPIA or not

Controllers should keep a record of their decision on whether to carry out a DPIA and rationale for their decision in line with the accountability principle. This is particularly important where they decide that a DPIA is not necessary. If available, attach other relevant documents that can help provide justification such as a project plan.

Please refer to section (b) of the Data Privacy Impact Assessment (DPIA) Template for Regulated Entities.

7.3. Provide details of the processing activity

Controllers should provide an explanation of the intended aim of their project and what forms of processing it will entail. Such details should include descriptions of:

- what will be processed - the personal data that will be processed, including any personal data of special nature;
- whose data will be processed - the individuals whose personal data will be processed;
- how the processing will take place - the nature of processing, for example, the frequency, systems used, processing location etc.; and
- why this processing will take place - the purpose of processing (for more see Permitted Reasons Guidelines for Regulated Entities).

Please refer to section (c) of the Data Privacy Impact Assessment (DPIA) Template for Regulated Entities.

7.4. Assess necessity and proportionality

Controllers are accountable for processing in compliance with the principles of the PDPPL including data minimisation and storage limitation.

Controllers should assess whether the personal data that will be collected are strictly necessary to achieve their intended purpose, an assessment of "necessity," and whether they could reasonably achieve their purpose for processing in another less intrusive or risky way, an assessment of "proportionality."

Controllers should include details of how they will ensure data protection compliance, which are a good measure of necessity and proportionality. In particular, controllers should include relevant details of:

- their permitted reasons for the processing;
- how they will prevent function creep;
- how they intend to ensure data quality;
- how they intend to ensure data minimisation;
- how they intend to provide privacy information to individuals;
- how they implement and support individuals' rights;
- measures to ensure their processors comply; and
- safeguards for international transfers.

Please refer to section (d) of the Data Privacy Impact Assessment (DPIA) Template for Regulated Entities.

7.5. Conduct risk assessment and identify risk mitigating actions

Controllers are accountable for protecting personal data, to demonstrate compliance they must identify and record the risks posed by the processing activity and the likelihood and impact of damage to individuals' privacy and personal data.

The risks controllers identify include those posed by a security breach affecting personal data but also risks relating to individuals' control over their personal data and privacy, for example, non-compliance with data protection principles such as data minimisation or purpose limitation.

Once controllers have identified the risks, they should decide on the appropriate measures needed to mitigate those risks. They should identify staff responsible for implementing each measure and they are implemented. Where appropriate, such measures may be embedded into risk response plans as part of the controller's existing risk and control framework.

Controllers should also identify the residual risk that will remain following implementation of their mitigation measures. If there is a high risk of serious damage that remains following the measures they have identified, controllers should consult the National Cyber Governance and Assurance Affairs on how to proceed.

Please refer to section (e) of the Data Privacy Impact Assessment (DPIA) Template for Regulated Entities.

7.6. Assess the potential for serious damage against measures identified

Controllers should be confident that the measures they identify to protect the personal data being processed are commensurate to the risk of serious damage to the individual's privacy or their personal data.

Controllers must set out how they have decided on the right balance between appropriate protection measures and the risk posed to individuals taking into account:

- leading practice including state of the art technology;
- the costs of implementation of various protection measures available;
- the nature, scope, context and purposes of processing (the "what," "who," "how" and "why" of processing); and
- the risk of serious damage to individuals.

Guidance on what may cause serious damage is available in section 3 "When should controllers perform a DPIA?" above.

For guidance on appropriate administrative, technical and financial measures please see the Data Privacy by Design and by Default Guidelines.

Please refer to section (f) of the Data Privacy Impact Assessment (DPIA) Template for Regulated Entities.

7.7. Assess how the controller will demonstrate adherence to PDPPL principles

Controllers should record how each of the data protection principles will be demonstrated by the decisions made in their DPIA. This will help them check if they have missed anything and clearly identify how the processing complies with the PDPPL.

For information on the principles for processing please see the Principles of Data Privacy Guidelines for Regulated Entities.

Please refer to section (g) of the Data Privacy Impact Assessment (DPIA) Template for Regulated Entities.

7.8. Sign off

The DPIA form should be signed-off by:

- the staff responsible for leading data protection;
- the head of the department or function that owns the activity; and
- the staff members who contributed to the DPIA.

It should be stored so that it can be accessed quickly if required, for example, in the event of a breach.

Please refer to section (h) of the Data Privacy Impact Assessment (DPIA) Template for Regulated Entities.

7.9. Actions following DPIA

Controllers should ensure that their mitigating actions are incorporated into the project plan and monitor their successful implementation.

If controllers decide that they are unable to mitigate a particular risk, either technically or due to cost constraints, they should consult with the National Cyber Governance and Assurance Affairs department.

Controllers should keep their DPIA under ongoing review and update it if the facts of the processing change by following the full DPIA process.

8. Appendix A - Example DPIA Triggers

Examples of activities that may trigger a DPIA are:

- Technology implementations or upgrades, for example:
  - implementing a new Customer Relationship Management (CRM) system or system upgrade;
  - retiring or modifying an existing legacy Enterprise Resource Management (ERM) system;
  - using a new third-party system provider such as changing a credit card payment machine provider;
  - collecting personal data in a new way;
  - storing or securing personal data in a new way; and
  - changing the systems used to collect personal data in any way.
- Changes to existing processes, for example:
  - processing personal data for a new use case or disclose it to a new third party;
  - changing an established process that involves personal data;
  - sharing data with a controller or processor; and
  - a decision to keep data for longer than designated in the retention schedule or as disclosed in a privacy notice.
- Changes to products or services, for example:
  - developing a new product or service offering;
  - using of existing personal data to improve upon a product or service offering;
  - collecting additional personal data to improve upon a product or service offering; and
  - sharing data with a new third party to support a product or service offering.

The above list is not exhaustive but serves to provide examples of where a DPIA would be required.

End of Document