State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

Special Nature Processing

PDPPL-02050215E

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-02050206E	Data Privacy Impact Assessment (DPIA) Guidelines 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 "Controller and Processor 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

- The purpose of these guidelines is to explain what categories of personal data constitute personal data of a special nature and the requirement for controllers to obtain permission to process such personal data from the Compliance and Data Protection (National cyber governance and assurance affairs) department under Article 16 of the PDPPL.
- Certain types of personal data, called personal data of a special nature, are subject to additional protection under the PDPPL because they are sensitive, and their misuse or unlawful disclosure will likely lead to serious damage to the individual.
- Personal data is considered of a special nature if it relates to ethnic origin, children, health, physical or psychological condition, religious creeds, marital relations, and criminal offences.
- Controllers must obtain the permission of the National cyber governance and assurance affairs to process personal data of a special nature for any purpose. To obtain permission they must:
    - Conduct a Data Protection Impact Assessment (DPIA) to identify the risks of processing and actions to mitigate those risks.
    - Identify both a permitted reason for processing and an additional condition for special nature processing and document these in their record of personal data processing.
    - Submit a request for permission to process special nature personal data to the National cyber governance and assurance affairs.
- If the National cyber governance and assurance affairs rejects a request to process personal data of a special nature, they will inform the controller of their decision along with recommended actions for the controller to implement before applying for permission again.
- Once permission has been granted for special nature processing the controller may only carry out the processing activity as set out in the application for permission. Any changes to processing will require an updated permission from the National cyber governance and assurance affairs.

2. Introduction

In order to provide certain products or services, controllers may need to collect or process certain types of personal data that are deemed more sensitive. The PDPPL refers to these categories of personal data as "personal data of a special nature," and they require additional protection due to their sensitive nature.

These guidelines have been prepared by the Compliance and Data Protection (National cyber governance and assurance affairs) Department to provide controllers with information on what constitutes personal data of a special nature and special nature processing, and what they should do if they plan to process such personal data. The requirements for special nature processing can be found in Article 16 and are explained in more detail below.

3. What does the PDPPL say about personal data of a special nature?

3.1. What does the PDPPL classify as personal data of a special nature?

Article 16 of the PDPPL states:

> *"Personal data with special nature includes data on **racial origin, children, health condition, physical condition, psychological condition, religious creeds, marital relations,***
>
> ***and crimes**.*
>
> *The Minister may add other types of Personal Data of a special nature where the misuse and/or disclosure of the same may cause **serious damage to individuals**…"*

Controllers should refer to this guidance regularly for updates, in case by virtue of a ministerial decision:

- Any other type of personal data is classified as special nature;
- There are any additional binding precautions for protecting personal data of a special nature.

3.2. What does the PDPPL say about permission for special nature processing?

Article 16 of the PDPPL says:

> *"Personal Data of a special nature may only be processed **after obtaining the permission from the Competent Department**, as per the measures and controls determined by a decision issued by the Minister.*
>
> *The Minister may, upon a decision therefrom, impose additional precautions with the intent of protecting Personal Data of a special nature."*

3.3. What does a controller need to do to comply with Article 16?

If a controller wishes to process personal data of a special nature, they should:

- Identify both a permitted reason for processing and an additional condition for processing. Controllers should ensure that they determine their condition for processing personal data of a special nature before they begin the processing, and they should document it in their records of personal data processing.
- Complete a DPIA (in line with Articles 11 and 13 of the PDPPL) as a processing activity that includes personal data of a special nature poses a higher likelihood of serious damage to individuals.
- Obtain permission from the National cyber governance and assurance affairs to process such personal data for the purpose the controller has identified.

To obtain permission from the National cyber governance and assurance affairs Controllers must demonstrate that they have a valid purpose for processing, have

identified an appropriate permitted reason and additional condition for processing, and have put in place appropriate administrative, technical and financial precautions to protect the personal data.

The National Cyber Security Agency may, via a ministerial decision, determine precautions that controllers will have to take to continue to lawfully process personal data of a special nature. This guideline will be updated if such a decision is taken by the Minister.

4. What is personal data of a special nature?

Personal data of a special nature includes the types of personal data that by its very nature, if misused, are more likely to result in serious damage to the privacy and / or personal data of individuals.

4.1 Why is it classified as "special nature"?

These types of personal data merit specific protection and should be handled with greater care because use of this data poses a greater risk to individuals and misuse or mishandling could result in greater damage to individuals than other categories of personal data or open an individual up to discrimination.

Whilst other personal data requires protection (such as an individual's net worth), this does not raise the same serious risks and so does not constitute personal data of a special nature as set out in the PDPPL.

4.2 What types of personal data are of a special nature?

As per the PDPPL and subsequent ministerial decisions, personal data relating to any of the below is considered as personal data of a special nature:

- Ethnic origin (race)
- Children
- Health, physical or psychological condition
- Religion
- Marital relations
- Criminal offences

It may be possible to infer or guess details of personal data of a special nature. Whether or not this constitutes personal data of special nature depends on how certain that inference is, and whether controllers are intent on drawing that inference. If information can be inferred that relates to one of the categories above with a reasonable degree of certainty, then it's likely to be personal data of special nature.

5 What are the additional conditions for processing personal data of special nature?

If controllers are processing personal data of a special nature, they need to identify both a permitted reason for processing and an additional condition for processing this type of data. Controllers should ensure that they determine their condition for processing personal data of a special nature before they begin this processing, and they should document it in their Record of Processing Activities (RoPA). Identifying such an additional condition is a condition for obtaining permission from the National cyber governance and assurance affairs. Below are the additional conditions:

- ***Explicit consent:*** the controller has obtained explicit consent from the individual to process such personal data, for which the nature and purpose for processing has been clearly disclosed to the individual.
- ***Parental consent:*** the controller has obtained explicit consent from the parent of the child to process such personal data, for which the nature and purpose for processing has been clearly disclosed to the child and parent.
- ***Made public by the data subject:*** the personal data in context is already made public by the individual and is only processed in that context and not processed for any other reason than that which it is collected.
- ***Employment:*** the personal data in context is that of the controller's employees or their immediate family and needs to be processed so that the controller can fulfil their obligations as an employer. Such obligations are defined in the employee's employment contract.
- ***Social security:*** the processing in context is necessary to maintain social security, that the controller is clearly obligated by appropriate legislative authority to maintain a level of social security.
- ***Vital interests:*** the processing in context is necessary to save an individual's life.
- ***Legal claims:*** the processing in question is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- ***Preventive or occupational medicine:*** the processing in context is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health care or treatment.
- ***Charity or not-for-profit administration:*** the processing in context is necessary for administering the affairs of a charity or not-for-profit organisation.
- ***Public health:*** the processing in context is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare.
- ***Public interest:*** the processing in context is necessary for reasons of substantial public interest with a basis in law.
- ***Protecting national and public security:*** the processing in context is necessary for the protection of national and public security with a basis in law.

6 What should controllers do before processing personal data of a special nature?

Before processing personal data of special nature, in addition to other requirements of the PDPPL, controllers need to take the steps listed below to ensure the additional layer of protection for such data.

6.1 Identify the additional condition for processing and update records of personal data processing

The permitted reason and additional condition for processing should be documented in their records of personal data processing, in line with the guidelines provided above. If the controller cannot identify the additional condition of processing the personal data of special nature, the processing activity will be deemed unlawful in line with the PDPPL and permission to process will not be granted.

6.2 Assess the risks to the special nature processing as part of a DPIA

As part of the DPIA (For more information, please refer to the Data Privacy Impact Assessment (DPIA) Guidelines for Regulated Entities) the controller needs to identify, at the time of designing the processing activity, whether they will be processing personal data of a special nature. They need to also identify the purpose and permitted reason of processing, the potential to cause serious damage to the individuals, risks to the processing and mitigating actions they will take to mitigate those risks. If they have identified a risk which they cannot sufficiently mitigate, they should consult the National cyber governance and assurance affairs before moving forward.

6.3 Request National cyber governance and assurance affairs for permission for the special nature processing

Once the controller has identified and documented their permitted reason and additional condition, completed their DPIA, and implemented the risk mitigation measures identified, they should apply for permission from the National cyber governance and assurance affairs for the special nature processing. Only once they have received such permission (or equivalent confirmation from the National cyber governance and assurance affairs) can their special nature processing be deemed lawful.

7 How can controllers request permission from the National cyber governance and assurance affairs to process personal data of special nature?

Controllers should apply for permission from the National cyber governance and assurance affairs by filling out and submitting the Special Nature Processing Request Form.

In addition to the form, the controller should provide:

- The DPIA conducted and signed off for this processing activity, with confirmation that the risk mitigation actions have been implemented.
- Any other additional information that the National cyber governance and assurance affairs requests.

The controller should ensure that they communicate regularly with the National cyber governance and assurance AFFAIRS and answer any questions the National cyber governance and assurance affairs may have while evaluating their request for permission. The National cyber governance and assurance affairs may also request further information related to the organisation and/or its key stakeholders.

7.1 What if a controller has already been processing personal data of a special nature?

At the time of enactment of the PDPPL, controllers might already be processing personal data of a special nature. Controllers should request permission for the ongoing processing from the National cyber governance and assurance affairs, using the same channel described above. If permission is not provided, the controller may be instructed by the National cyber governance and assurance affairs to cease processing until permission has been obtained.

7.2 What if the National cyber governance and assurance affairs rejects the controller's request for processing personal data of a special nature?

If the National cyber governance and assurance affairs rejects a controller's request for permission to process personal data of a special nature, the National cyber governance and assurance affairs will inform the controller of this decision. In this communication, the National cyber governance and assurance affairs will state the reason why the request was rejected and will provide recommended actions for the controller to implement, if applicable. The controller can request for permission from the National cyber governance and assurance affairs again after implementing these actions. Note that in such cases, the processing of personal data of a special nature will only be lawful after obtaining permission from the National cyber governance and assurance affairs.

8 Appendix A - Special Nature Processing Checklist

This checklist is meant to help controllers identify whether they process personal data of special nature and (if they do) if they have a valid additional condition for processing.

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

☐ We are aware of whether we are processing personal data of a special nature.

- We are aware of the personal data types that are deemed to be of a special nature, as determined by the National cyber governance and assurance affairs Department via the PDPPL and any further ministerial decree. Below are the personal data types:
    - Ethnic origin (race)
    - Children
    - Health, physical or psychological condition
    - Religion
    - Marital relations
    - Criminal actions / crimes

☐ We have identified and listed our processing activities that process personal data of a special nature in our Records of Processing Activities.

- For existing processing activities, we have made a list of these processing activities in our records of personal data processing, along with the personal data type that is processed.
- For all new processing activities, as part of a DPIA, we will assess if we will process personal data of a special nature.

☐ We have checked if the processing of the personal data of a special nature is necessary for the purpose we have identified and are satisfied there is no other reasonable and less intrusive way to achieve that purpose.

☐ Where we process personal data of a special nature, we have identified and documented an additional condition for processing.

- We are not processing personal data of a special nature without one or more of the following additional conditions:
    - ***Explicit consent:*** the controller has obtained explicit consent from the individual to process such personal data, for which the nature and purpose for processing has been clearly disclosed to the individual.
    - ***Parental consent:*** the controller has obtained explicit consent from the parent of the child to process such personal data, for which the nature and purpose for processing has been clearly disclosed to the child and parent.

- ***Made public by the data subject:*** the personal data in context is already made public by the individual and is only processed in that context and not processed for any other reason than that which it is collected.
- ***Employment:*** the personal data in context is that of the controller's employees or their immediate family and needs to be processed so that the controller can fulfil their obligations as an employer. Such obligations are defined in the employee's employment contract.
- ***Social security:*** the processing in context is necessary to maintain social security, that the controller is clearly obligated by appropriate legislative authority to maintain a level of social security.
- ***Vital interests:*** the processing in context is necessary to save an individual's life.
- ***Legal claims:*** the processing in question is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.
- ***Preventive or occupational medicine:*** the processing in context is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health care or treatment.
- ***Charity or not-for-profit administration:*** the processing in context is necessary for administering the affairs of a charity or not-for-profit organisation.
- ***Public health:*** the processing in context is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare.
- ***Public interest:*** the processing in context is necessary for reasons of substantial public interest with a basis in law.
- ***Protection national and public security:*** the processing in context is necessary for the protection of national and public security with a basis in law.

☐ We have sought and obtained permission from the National cyber governance and assurance affairs Department to process such sensitive personal data.

- Before we commenced processing sensitive data, we applied to the National cyber governance and assurance affairs Department for permission via the appropriate channel and furnished the required documents and information. We also furnished evidence that:
  - We conducted a DPIA before implementing the processing activity, where the risks related to processing were identified and mitigating actions agreed on.
- Where the National cyber governance and assurance affairs reverted asking for additional security measures to be implemented, we designed

and implemented those security measures before we commenced processing of the personal data.

☐ We include specific information about our processing of personal data of a special nature in our privacy notice to individuals.

☐ We have implemented a Personal Data Management System (PDMS) in line with the PDPPL, thereby demonstrating that we protect personal data (whether of a special nature or not) that we process to the most reasonable extent possible.

End of Document