



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency




PDPPL Working Groups – PDPPL and the Role of the NDPO

14th – 18th May 2023

→ www.ncsa.gov.qa

Objectives of the Working Groups

Demonstrated below is the aim, scope and objectives of the PDPPL working groups:

<p>Aim</p> 	<p>The Personal Data Privacy Protection Law (PDPPL) Sectoral Working Group is a standing committee established to identify initiatives to promote PDPPL compliance and foster engagement between the NDPO and controllers of personal data within sectors.</p>
<p>Scope</p> 	<p>The scope of the group is limited to the activities described in the aim and the areas of focus below in relation to the PDPPL:</p> <ul style="list-style-type: none">• provide industry stakeholders with an avenue to communicate with the National Data Privacy Office (NDPO) regarding key issues within the Sector;• highlight technological and privacy-related developments in the Sector that may require NDPO consideration; and• identify topics for guidance and information that would support organisations within the Sector in their endeavours to comply with the PDPPL.
<p>Objectives</p> 	<ul style="list-style-type: none">• NDPO to communicate key messages to the sector identified through its work as the regulator• Organisations to share insight into common challenges facing organisations in the sector in relation to the PDPPL and data privacy.• NDPO to capture areas for focus within the sector to support compliance.• Organisations to receive guidance in response to questions and queries.

National Context

HH the Amir Sheikh Tamim bin Hamad al-Thani issued Law No 13 of 2016 on protecting personal data also known as the “Personal Data Privacy Protection Law” or “PDPPL”. This makes Qatar the first country in the GCC to have a law dedicated to data protection.

The PDPPL is a natural evolution of key statements relating to privacy within the Qatari Permanent Constitution, QNV2030 and Qatar’s National Cyber Security Strategy (passed by the MOTC in 2014). The next step in this journey is to setup the Regulator to enforce the PDPPL, as well as control related documentation and provide guidance related to the PDPPL to organisations and individuals in Qatar. This regulator is the NDPO.



The issuing of the PDPPL made Qatar the first country in the GCC to pass a law dedicated to the protection of personal data. It reinforces Qatar’s commitment to ensuring a safe environment for its citizens and residents, by mandating that organisations protect the personal data of individuals that they collect and process.



2004: Qatar Permanent Constitution

“The sanctity of human privacy shall be inviolable, and therefore interference into privacy of a person, ...”



2008: Qatar National Vision 2030

- “Human Development: Development of all its people to enable them to sustain ...”



2014: Qatar Cyber Security Strategy

“The Qatari government shall... enact proposed laws (e.g. Data Privacy and Protection Law...”

Key Areas of PDPPL

Organisations in Qatar that process personal information of individuals need to comply with the PDPPL and some of the key areas of the law are provided below. Organizations can refer to the guidance provided by the NDPO for effective compliance with the law.



Principles of PDPPL



Privacy Notice



Permitted Reasons



Special Nature Processing



Individuals' Rights



Data Processor Obligations



Direct Marketing Requirements



Children's Data Management



Personal Data Breach Management



Personal Data Management Standard



Security for Privacy



Records of Processing Activities

PDPPL Principles

Most data privacy laws are built on a set of key principles, which establish the foundation for everything related to data privacy and the protection of personal data. PDPPL lists out seven key data privacy principles that form the fundamental conditions that organisations must follow when processing personal data. Processing personal data in line with these key principles is essential.



Transparency, honesty and respect for human dignity

You should always process personal data in a transparent, honest and respectful manner, in line with the requirements of the applicable data privacy laws.



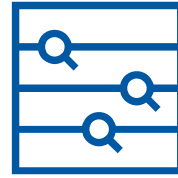
Purpose Limitation

You should only process personal data for a specified and lawful purpose. You cannot use the data for another purpose unless conditions are met.



Data Minimisation

You must ensure you are only processing the personal data which you truly need to conduct your business and nothing more.



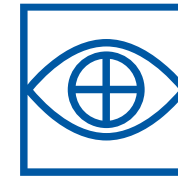
Accuracy

You should ensure personal data is kept up to date, and that necessary measures are in place for correcting and updating inaccurate data.



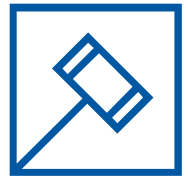
Storage Limitation

You must not keep personal data for longer than you need it. It should be securely destroyed after the defined retention period.



Integrity & Confidentiality

You must implement adequate security controls to ensure that personal data is protected against loss, destruction or damage.



Accountability

You must have appropriate measures and records in place to be able to demonstrate your compliance.

Guidelines for Organisations

We are here to offer advice and guidance, promote good practice, carry out audits and advisory visits, consider complaints, monitor compliance and support enforcement action where appropriate. Below are key guidelines that you can use to support your compliance initiatives.

Key guidelines for controllers and processors



Permitted Reasons



Privacy Notice



Competent Authority
Exemptions including Records



Data Protection Self-Assessment



Individuals' Rights



Breach notifications



Controller Exemptions



Internal Communications
Guidance



DPIA Guidelines & Template



Controller and Processor
Guidelines incl. Contracts



Electronic Direct Marketing



Data Privacy By Design & Default



Individuals' Complaints



Principles of Data Privacy



Special Nature Processing
Guidelines & Checklist



Records of Processing Activities
(RoPA)



Personal Data Management
System (PDMS) Checklist

What these guidelines do

- Support organisations in understanding their obligations
- Provide a degree of clarity around these requirements as well as checklists and template documents to support the compliance of the PDPPL
- Provide templates and examples to support on a compliance journey.

What these guidelines do not do

- Tell you exactly what you need to do
- Make decisions for you on how you process personal data.
- Make a decision for you about whether you are in scope or not

Permitted Reasons for Processing

When can personal data be processed?



What are the exemptions?

Exemptions for competent authorities	Exemptions for controllers
<ul style="list-style-type: none">• To ensure national security, law and order; or• To protect international relations of the State of Qatar; or• To safeguard the economic or financial interests of the State of Qatar; or• To prevent, gather information about or investigate a crime.	<ul style="list-style-type: none">• To execute a public interest based task, as per applicable law; or• To enforce a legal obligation or an order from a competent court;• To protect the vital interests of an individual; or• To achieve a public interest based scientific research purpose; or• To collect personal data for a criminal investigation upon an official request from the investigating authority.

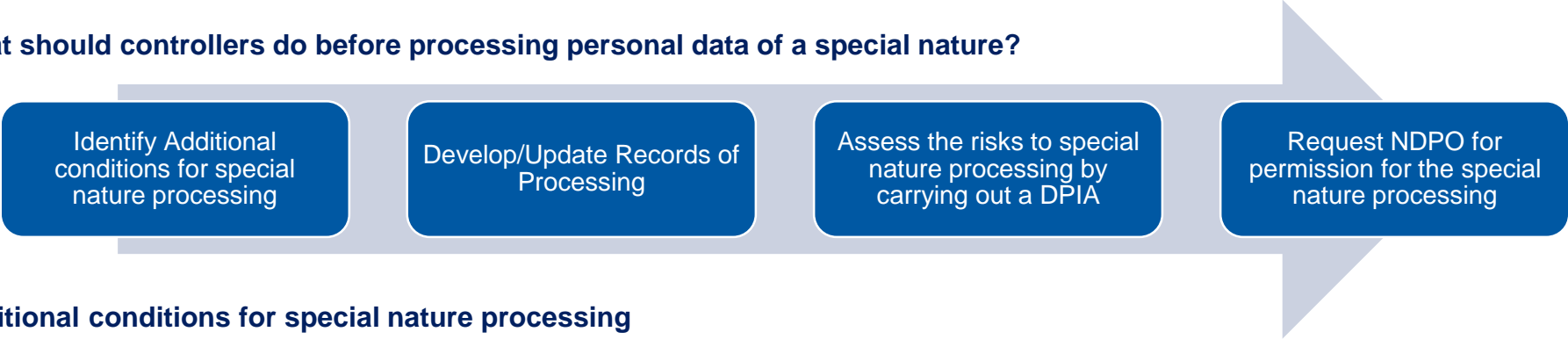
*Note: Categories of lawful purpose are yet to be formally published in the form of President Decision and corresponding guidelines as we are awaiting requisite approvals.

Special Nature Processing


What are Personal Data of a Special Nature?

Personal Data of Special Nature are the type of personal data that are associated with a higher risk; where misuse and/or disclosure of this data may cause serious damage to Individuals.

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



Additional conditions for special nature processing



Explicit Consent



Employment




Social Security



Vital Interests



Made Public by the Data Subject



Legal Claims










Preventive or Occupational Medicine



Public Health

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

-  Ethnic origin (race)
-  Children's data
-  Health, physical or psychological condition
-  Religion
-  Marital status
-  Criminal records
-  Biometrics

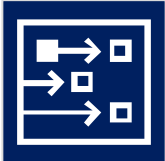
Individual's Rights

One of the aims of data privacy laws is to empower individuals and give them control over their personal data. Therefore, the PDPPL introduces what are usually referred to as 'Individual's right's concerning the protection of individual's personal data. It's important to note that not all of these rights are 'absolute', meaning some only apply in specific circumstances:



The right to protection and lawful processing

Individuals have the right to have their personal data protected and lawfully processed.



The right to withdraw consent

An Individual may withdraw their previously given consent.



The right to erasure

Individuals can have their personal data deleted without undue delay.



The right to object

Individuals have the right to object to the processing of their personal data.



The right to request correction

Individuals have the right to request that you correct the personal data you hold about them.



The right to be notified of processing

Individuals have the right to be informed about the collection and use of their personal data.



The right to be notified of inaccurate disclosure

Individuals have the right to be notified when inaccurate information has been shared with a third party and for such inaccurate disclosure to be corrected.



The right to access

Individuals have the right to obtain a copy of the personal data held on them.

Risk-Based Approach

The risk-based approach means that organisations should base decisions about how they process personal data on the risk of serious damage to individuals that may be caused by their processing activities. Organisations should decide on what administrative, technical and financial precautions are appropriate using an assessment called a Data Protection Impact Assessment (DPIA) that enables them to identify risks and decide appropriate mitigating precautions to protect the personal data being processed.

What does may cause serious damage mean?

Before processing personal data you should assess whether serious damage could be caused to the individual's privacy or personal data. There are many activities that may cause serious damage and this concept is address in detail in the DPIA guidelines. There are three instances that the PDPPL refers to that may cause serious damage specifically. These are:

Transferring personal data outside the State of Qatar, known as a cross-border data transfer.

Processing personal data of a special nature, specific categories of personal data also known as sensitive personal data.

Breaches of security or appropriate measures that could lead to unauthorised access to data or use that is not compliance with the PDPPL.

How do organisations determine what measures are appropriate?

Organisations must balance that administrative, technical and financial measures for data protection are appropriate for the risk of serious damage to individuals' personal data or their privacy. They should assess this during a DPIA in compliance with Data Protection by Design and Default guidelines.

Administrative, technical and financial measures must be put in place to process personal data is processed

- Securely
- In line with the principles
- Whilst giving individuals control

The Role of the NDPO

The NDPO acts as the PDPPL regulator and the custodian of the PDPPL, and is empowered to do so by a President Decision. As a regulator the NDPO has the mandate to supervise, regulate and develop Data Privacy in the State of Qatar. Below are the roles that the NDPO plays with regard to the PDPPL regulation. Some of the NDPO key responsibilities are set out below.



Establish and implement privacy guidelines, standards, policies and certifications as required



Coordinate with sector regulators and professional groups to implement DP laws and regulations.



Conduct research relating to the matters provided for in data protection regulations.



Issue guidance and develop awareness of PDPPL requirements in Qatar.



Receive data breach notifications and conduct investigations into potential PDPPL violations



Grant permission for processing of personal data of special nature



Investigate violations and recommend enforcement to appropriate legal authorities for PDPPL breaches.



Represent Qatar within the international data protection community.

Legal enforcement steps

The NDPO, in conjunction with the Public Prosecutor, has the ability to conduct investigations, supervisory visits and issue enforcement actions if a controller is found to be in breach of the PIPPL; the NDPO conducts these investigations and enforcement actions through the following steps:





الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Thank You

Email: privacy@ncsa.gov.qa

Website: www.ncsa.gov.qa

P.O. Box: 24100, Wadi Al Sail
Street, Doha – State of Qatar