



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

International Privacy Day Event

January 28th 2025



Introduction

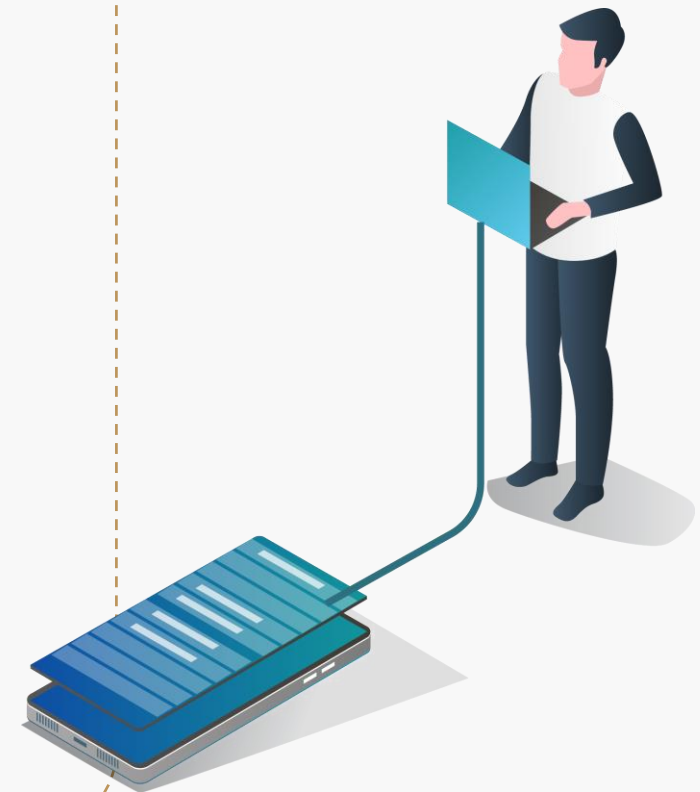
- Privacy is a fundamental right. This means that the right to privacy derives from the constitution of Qatar.
- Furthermore, the Law No. 13 for the year 2016 the Personal Data Privacy Protection Law also known as the PDPPL sets out obligations for entities that process personal data to protect the individual privacy.
- These obligations are mandatory whenever personal data is being processed, and they must be taken into consideration by all entities, **controllers** and **processors** alike.
- In this presentation we will go through the following:
 - › Information about the National Data Privacy Office
 - › What different definitions the PDPPL has and why they are important
 - › What obligations does the PDPPL have for controllers
 - › What individual rights does the PDPPL include
 - › Q&A section at the end where you can ask us questions about the presentation.





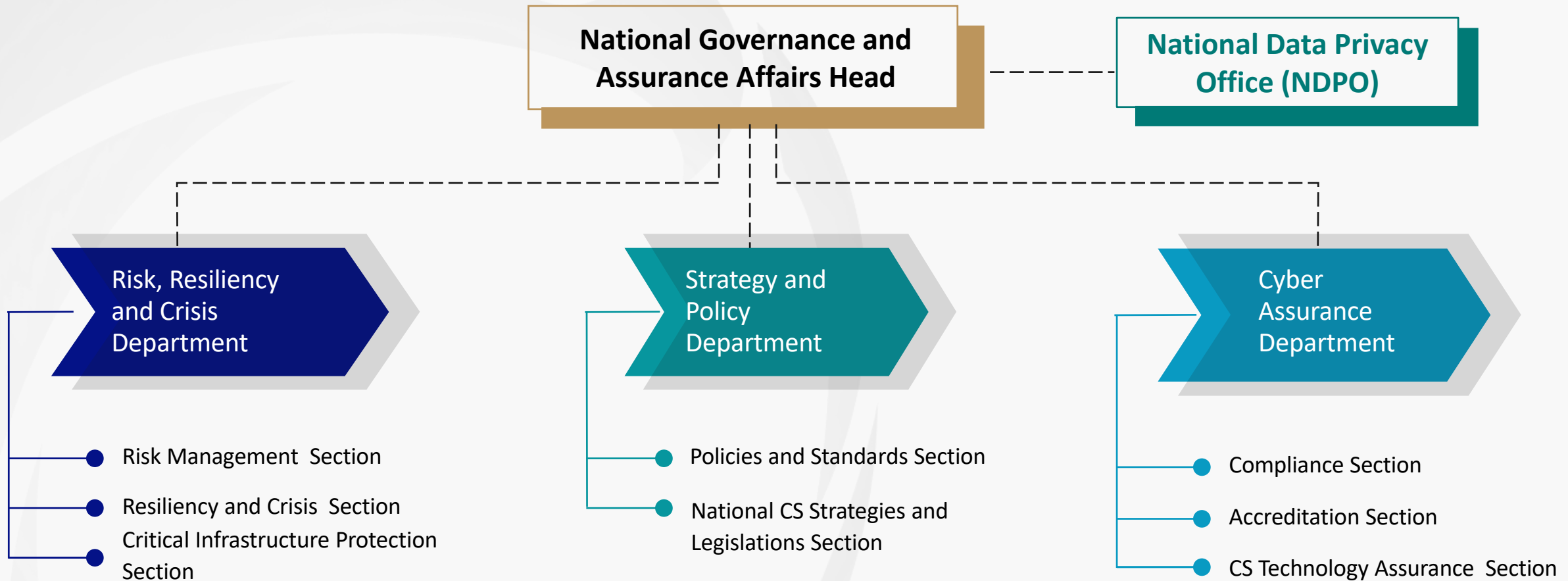
NDPO

- The National Data Privacy Office (NDPO) acts as **regulator** for the Law No. 13 for the year 2016, the Personal Data Privacy Protection law (the PDPPL) regulator
- Offers advice and guidance, promotes good practices, monitors compliance, and supports enforcement action
- Aims to increase awareness of privacy rights of the individuals provided by the PDPPL and controller's obligations derived from the PDPPL directed at all entities processing personal data.





Organization's Structure





The Role of the NDPO

The NDPO acts as the PDPPL regulator and the custodian of the PDPPL. As a regulator the NDPO has the mandate to supervise, regulate and develop Data Privacy in the State of Qatar. 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.



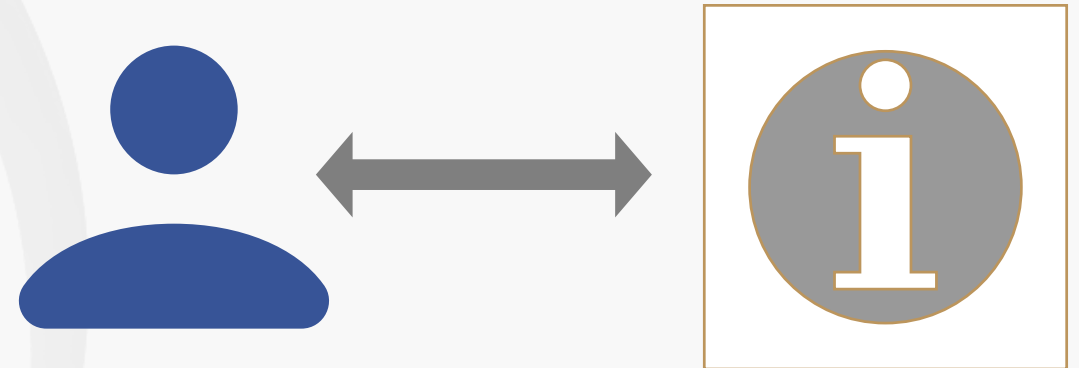
Represent Qatar within the international data protection community.



Definitions – What is Personal Data? (PDPPL Art. 1)

Personal data: Data of an individual whose identity is defined or can be reasonably defined whether through such personal data or through the combination of such data with any other data. e.g. name, date of birth, phone number, video, email address, IP address, behavioral data, pseudonymized data.

PDPPL applies.





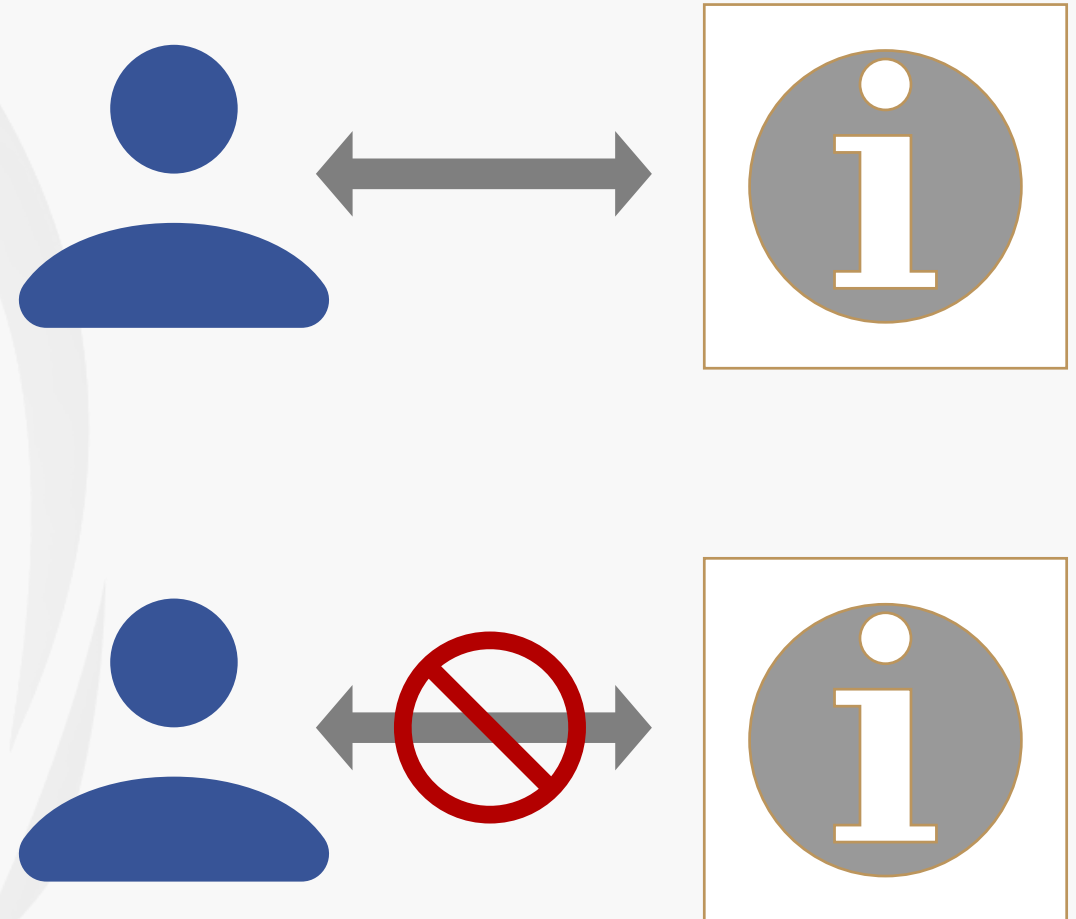
Definitions – What is Personal Data? (PDPPL Art. 1)

Personal data: Data of an individual whose identity is defined or can be reasonably defined whether through such personal data or through the combination of such data with any other data. e.g. name, date of birth, phone number, video, email address, IP address, behavioral data, pseudonymized data.

PDPPL applies.

Anonymized data: Data that cannot be connected to an individual by itself or when combined with other data.

PDPPL does not apply.





Definitions – What is Processing Personal Data? (PDPPL Art. 1)

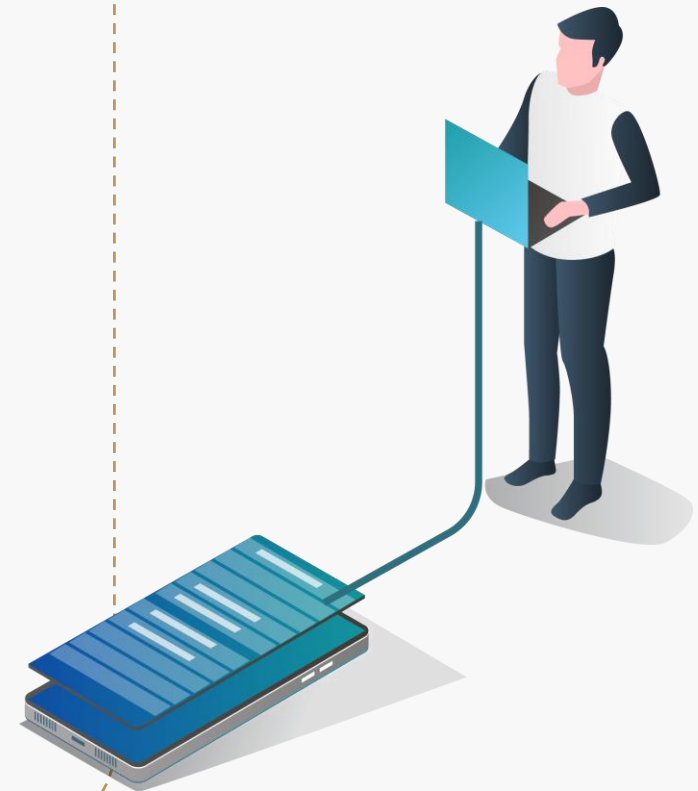
Processing Personal Data: Personal data processing through one or more operations.

Examples:

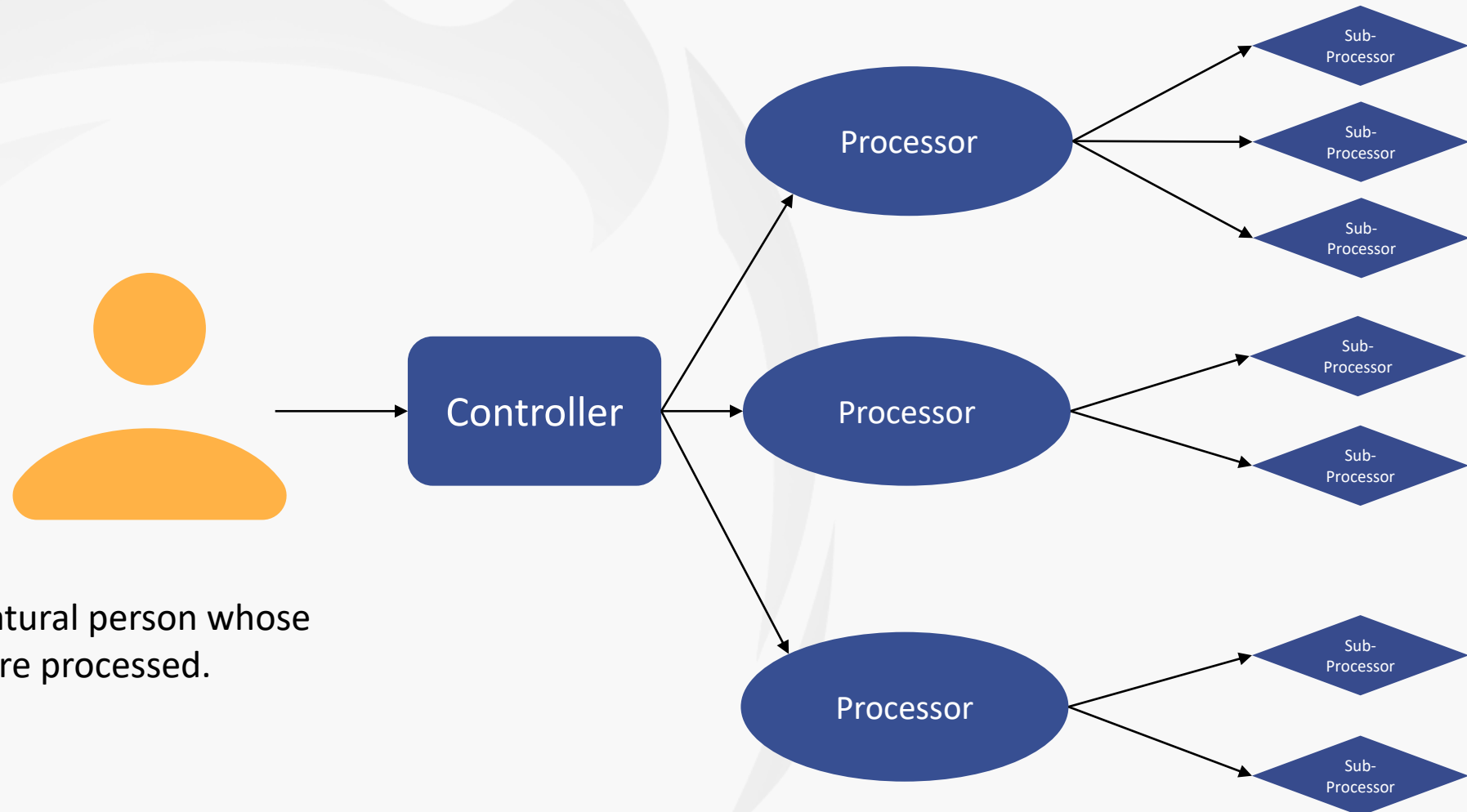
Collecting
gathering,
receiving,
registering,
organizing,
storing,

viewing,
modifying,
retrieving,
using,
disclosing,
publishing,

transferring,
withholding,
destroying,
anonymizing,
and combining.



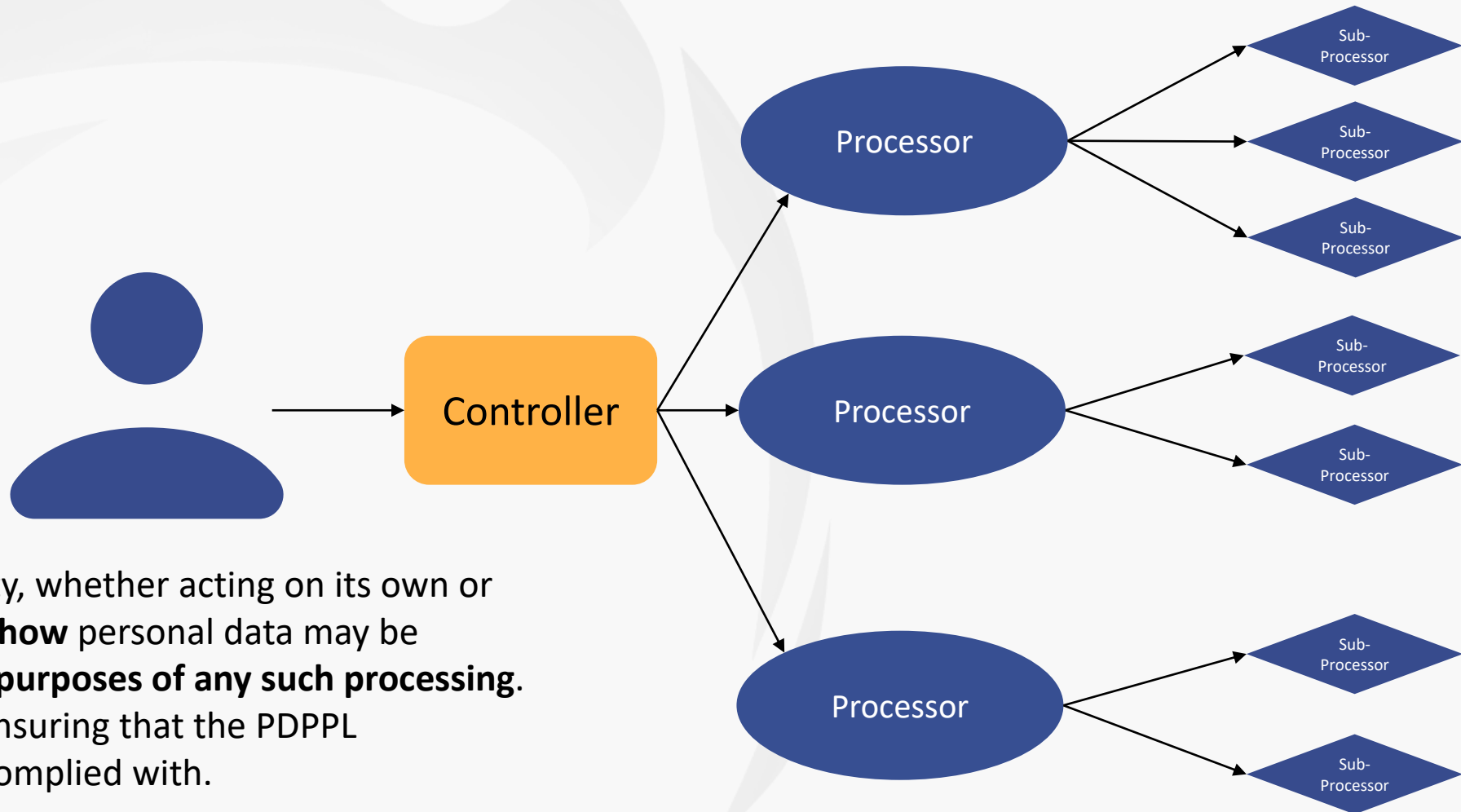
Definitions – Different Roles? (PDPPL Art. 1)



Individual: A natural person whose personal data are processed.



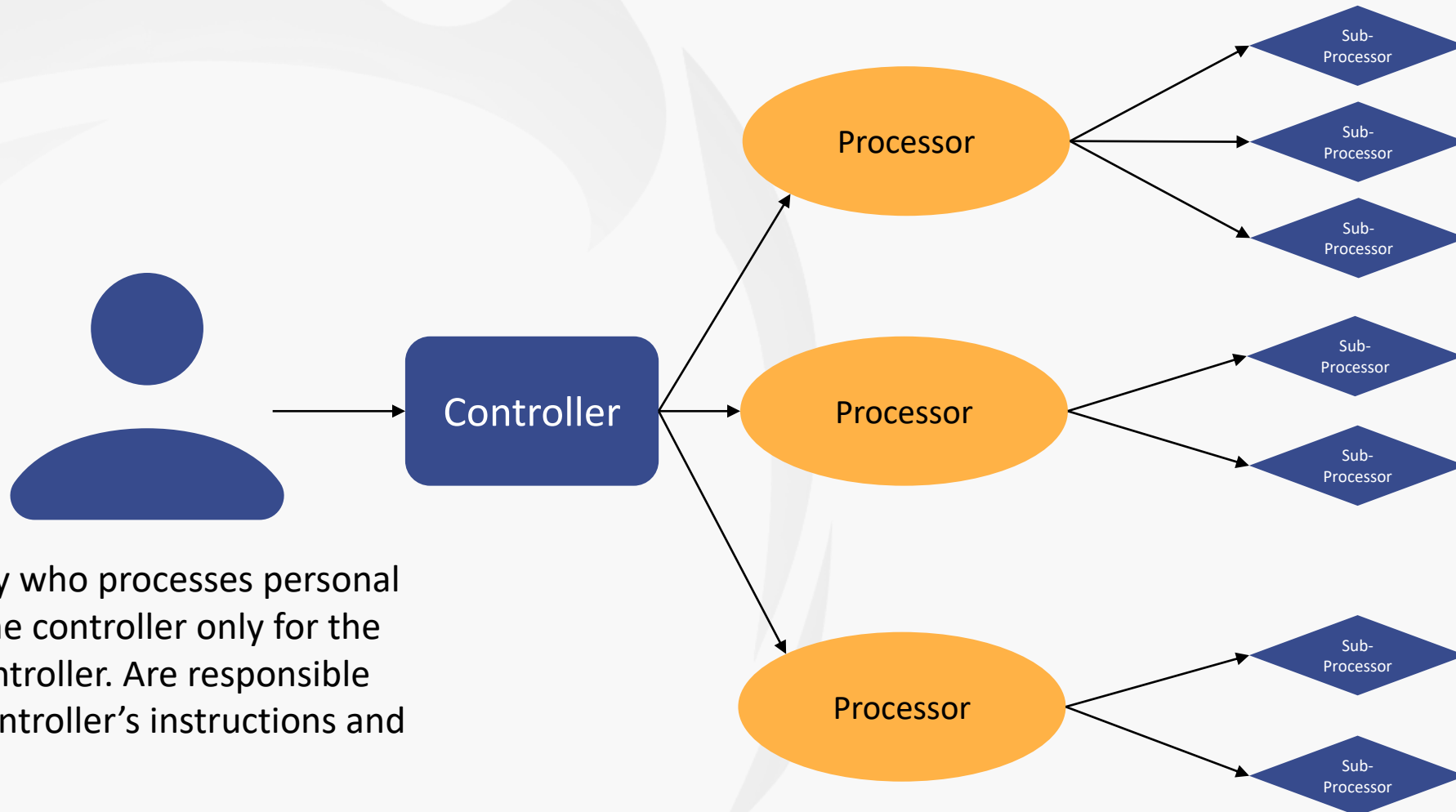
Definitions – Different Roles? (PDPPL Art. 1)



Controller: An entity, whether acting on its own or jointly, determines **how** personal data may be processed and **the purposes of any such processing**. Is responsible for ensuring that the PDPPL requirements are complied with.



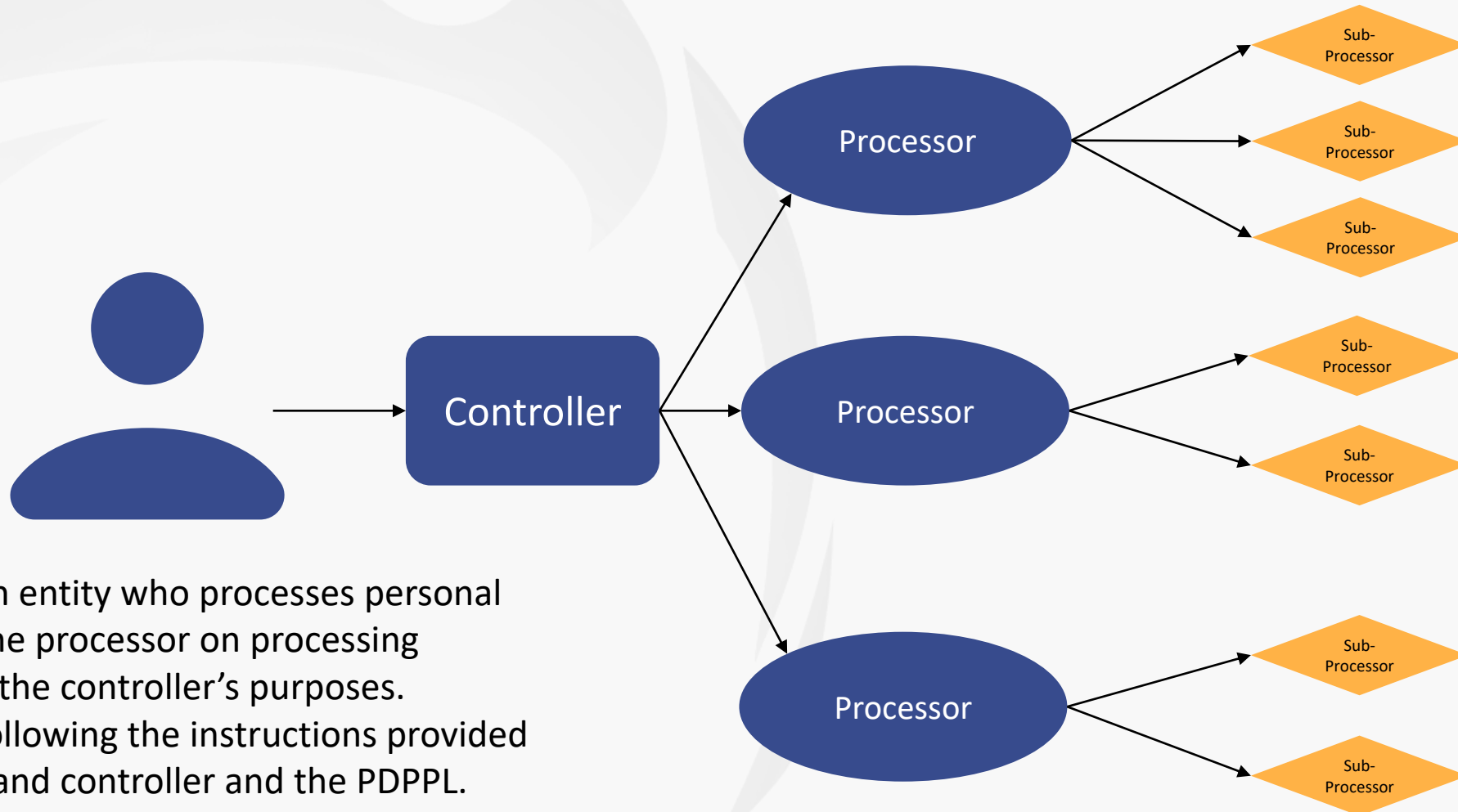
Definitions – Different Roles? (PDPPL Art. 1)



Processor: An entity who processes personal data on behalf of the controller only for the purposes of the Controller. Are responsible for following the controller's instructions and the PDPPL.



Definitions – Different Roles? (PDPPL Art. 1)



Sub-processor: An entity who processes personal data to support the processor on processing personal data for the controller's purposes. Responsible for following the instructions provided by the processor and controller and the PDPPL.

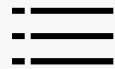


Structure of the PDPPL

The PDPPL is organised into the following chapters:



Chapter 1 (Articles 1-2): Definitions and Scope



Chapter 3 (Articles 8-15): Liabilities of Controller and Processor



Chapter 2 (Articles 3-7): Rights of Individuals



Chapter 4 (Articles 16-17): Personal Data of a Special Nature



Chapter 5 (Articles 18-21): Exemptions



Chapter 7 (Articles 23-25): Penalties



Chapter 6 (Article 22): Electronic Communication for the Purpose of Direct Marketing



Chapter 8 (Articles 26-32): Final Provisions



Key Areas of the 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 the 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 organizations 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.



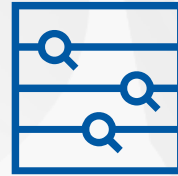
Purpose Limitation

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.



Permitted Reasons for Processing

When can personal data be processed?



Explicit Consent

of the individual to the processing of personal data.



Contractual

processing is needed to enter a contract.



Legal Obligation

for which the organisation is obliged to process data for.



Legitimate Interest

of the organisation or the third parties engaged.

What are the exemptions?

Exemptions for competent authorities

- 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.

Exemptions for controllers

- 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.



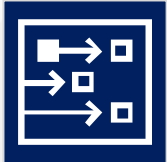
Rights of the Individual

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 rights concerning the protection of the 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 access

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



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 protection and lawful processing

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



Special Nature Processing

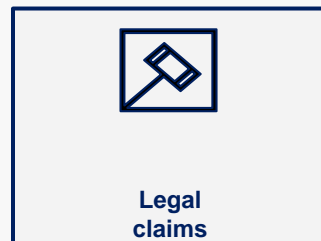
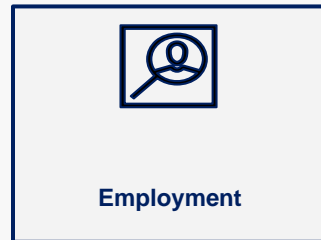
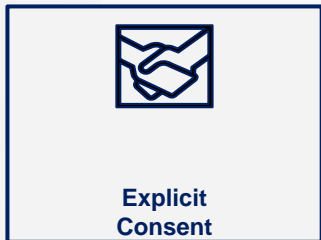
What are Personal Data of a Special Nature?

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.

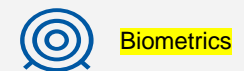
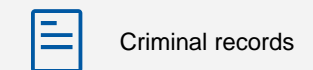
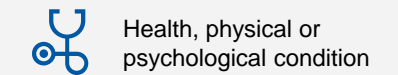
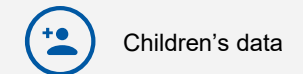
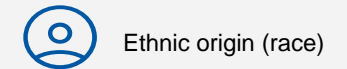
What should controllers do before processing personal data of a special nature?



Additional conditions for special nature processing



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





What is a Personal Data Breach

A personal data breach means a breach of security leading to the unlawful or accidental alteration, destruction, loss, unauthorized disclosure of, or access to, personal data. This includes both accidental and deliberate breaches.

Examples of Data breaches:

- Theft or loss of IT equipment containing personal or business sensitive data.
- Inappropriately accessing personal data about customers/staff.
- Leaving confidential / sensitive files that may contain personal data unattended.
- Inadequate disposal of confidential files that may contain personal data material.
- Unauthorized disclosure of client data.
- Using client data for personal gain.

Adverse Impact of Data Breaches

Personal data breaches often result in adverse impact(s) being suffered by individuals, organizations and/or communities, such as:

- Compromised personal safety or privacy.
- Burden of additional legal obligation(s) or regulatory penalty(ies).
- Financial loss / commercial detriment.
- Disruption to business or reputational damage.
- Inability of individuals to access their data or exercise rights under privacy laws.



Controller Requirements for Data Breaches

Controllers should implement appropriate safeguards to prevent data breaches and notify data breaches if the breach may cause serious damage to individuals' privacy. Controllers are required to determine if the breach may cause serious damage through an assessment.

Implement Appropriate Safeguards

Controllers should take appropriate precautions to prevent and reduce the likelihood and impact of breaches.

Detect breaches

Controllers should be able to detect a breach if it occurs and immediately assess the potential for serious damage to individuals.

Notify personal data breaches to the NDPO

Controllers should report the personal data breach to the National Data Privacy Office without delay and within 72 hours of becoming aware of it, if the personal data breach could cause damage to individuals' personal data or privacy.

Notify personal data breaches to the affected individuals

Controllers should notify the individuals of the personal data breach without delay and within 72 hours of becoming aware of it if the personal data breach could cause serious damage to their personal data or privacy.

NDPO

How to Notify?

Controllers should notify the National Data Privacy Office using the Breach Notification Form.

What to Notify?

- detail the nature of the personal data breach,
- include the name and contact details of the company's primary responsible person for privacy related matters
- describe the consequences likely to occur due to the personal data breach; and
- describe the action(s) that the controller has taken or proposes to take to address the personal data breach, including, where appropriate, actions to mitigate the possible adverse effects of the personal data breach.

Individuals

How to Notify?

The communication to the individual should be made directly to them and describe nature of the personal data breach in clear and plain language. Notification of affected individuals is particularly important when the breach could cause serious damage to the affected individuals' privacy or personal data.

What to Notify?


















- the name and contact details of the primary responsible person for privacy related matters
- a description of the consequences likely to occur due to the personal data breach; and
- a description of the action(s) that the controller has taken or proposes to take to address the personal data breach, including, where appropriate, actions to mitigate the possible adverse effects of the personal data breach.



Guidelines for the Organizations

The NDPO offers advice and guidance, promotes good practice, carries out audits and advisory visits, considers complaints, monitors compliance and supports enforcement action where appropriate. Below are key guidelines to support organizations in their 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



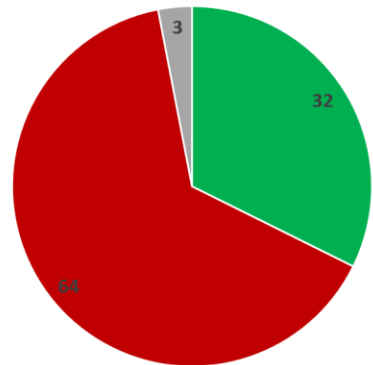
NDPO Privacy Compliance Assessment Tool

COMPLIANCE DASHBOARD

COMPLIANCE STATUS ACROSS DOMAINS

■ Compliant ■ Non Compliant ■ Not Applicable

Overall Compliance State



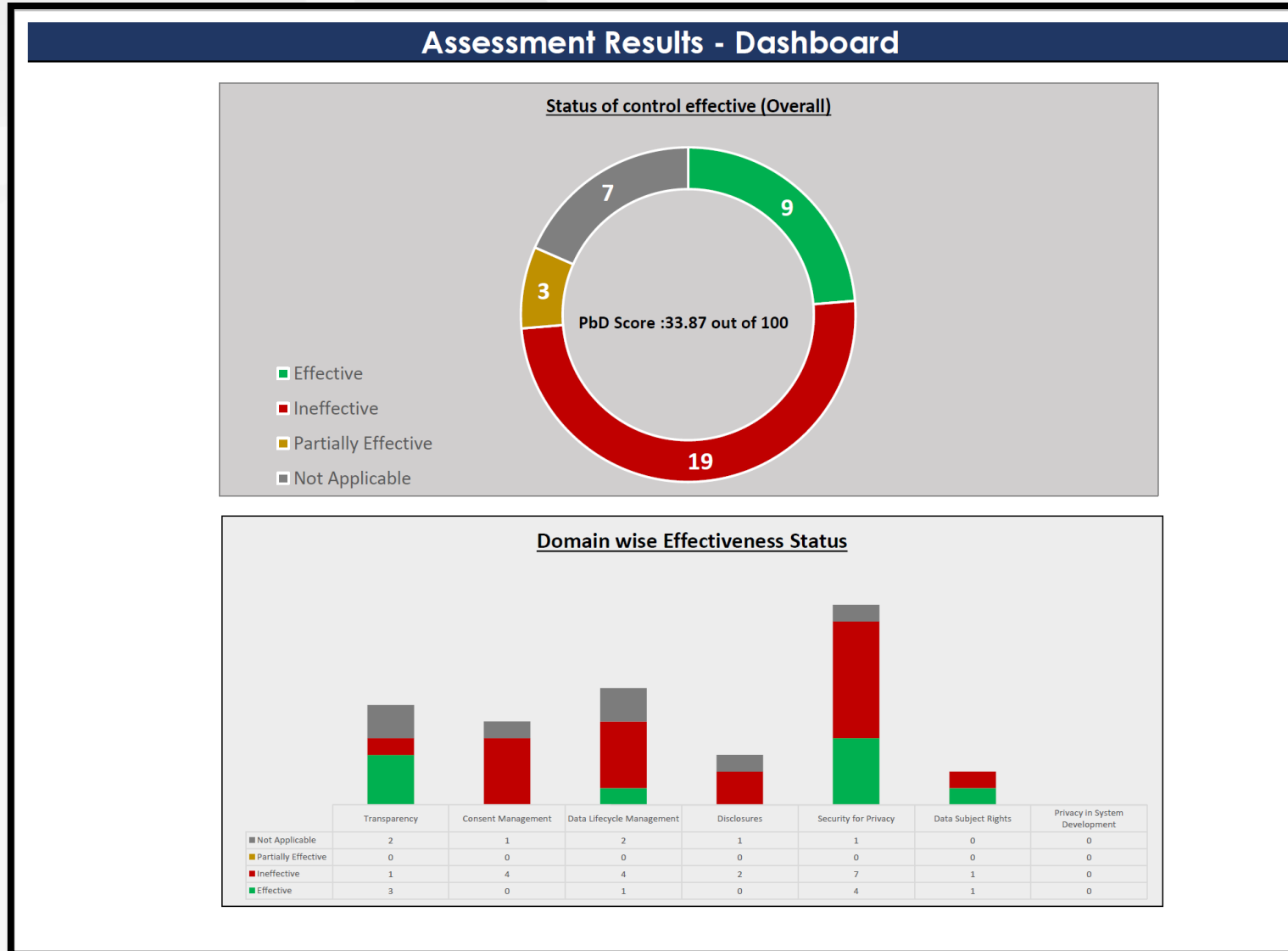
■ Compliant ■ Non Compliant ■ Not Applicable



	Privacy Governance	Transparency	Permitted Reasons	Special Nature Processing	Data Lifecycle Management	Individuals' Rights	Personal Data Breach Management	Disclosure to Third Parties	Direct Marketing	Privacy by Design	Security for Privacy	Continuous Compliance
Compliant	1	2	3	4	2	4	4	2	2	3	3	2
Non Compliant	2	5	6	7	5	8	6	4	5	6	7	3
Not Applicable	3	0	0	0	0	0	0	0	0	0	0	0



NDPO Privacy by Design Assessment Tool





الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Thank You

Email: privacy@ncsa.gov.qa

Website: assurance.ncsa.gov.qa

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



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency



International Data Privacy Event Building a Privacy Program (Workshop)



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Privacy Program: An Introduction

What is a Privacy Program?

A Privacy Program is a structured framework that helps organizations manage personal data responsibly and comply with privacy regulations and best practices. It involves establishing a governance structure, assessing data processing activities, implementing necessary controls, and ensuring ongoing compliance through monitoring and training.

Objectives of the Privacy Program

- **Achieve Regulatory Compliance:** Ensure adherence to Qatar's PDPPL and other applicable privacy regulations.
- **Reduce 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 privacy practices into business processes to optimize personal data management.
- **Foster a Privacy-Aware Culture:** Promote awareness and responsibility across all levels of the organization.



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Building Blocks of an Effective Privacy Program

An ideal Privacy Program should be composed of the below four phases that provide a structured approach to achieving and maintaining compliance with privacy regulations.

I

Establish a Privacy Blueprint

Build the foundation for privacy governance by defining the privacy vision, mission, and establishing roles and responsibilities to oversee initiatives.

II

Assess Current Practices

Evaluate the privacy posture by identifying personal data processing activities, assessing compliance against regulatory requirements, and developing a roadmap for improvement.

III

Implement Privacy Requirements

Operationalize privacy requirements through the development of policies, managing data lifecycles, providing privacy notices, obtaining consent, handling individual rights, data breaches, etc.

IV

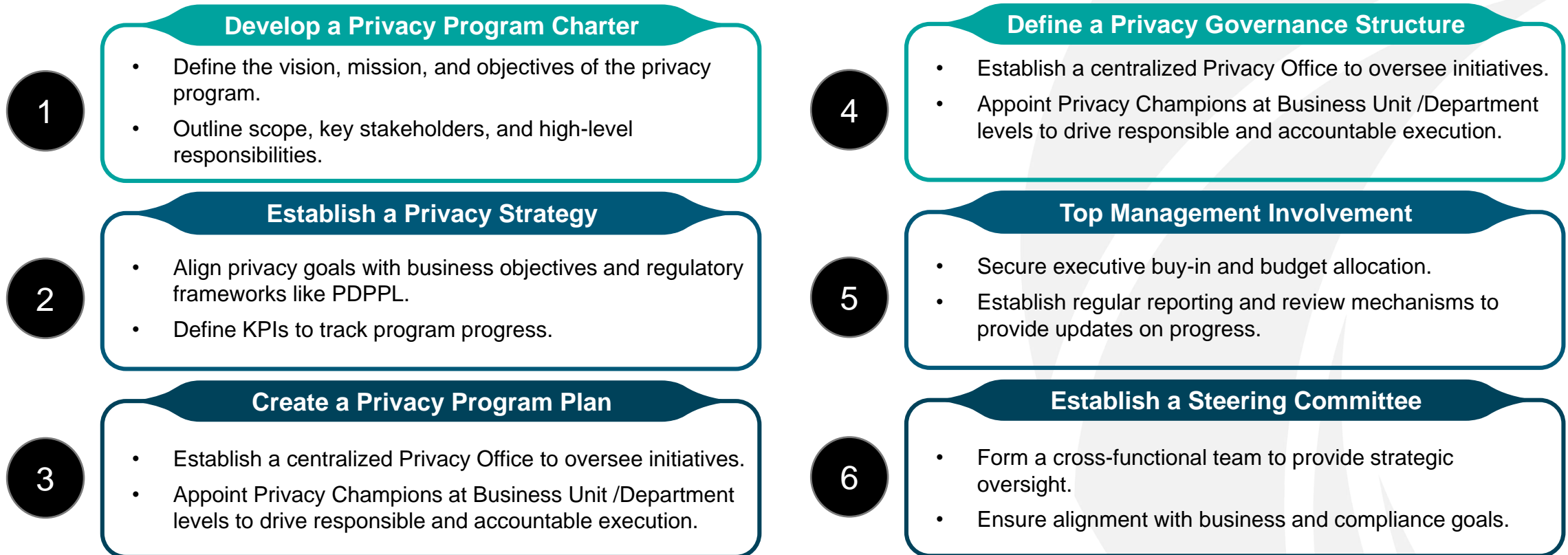
Sustain and Improve Compliance

Ensure continuous compliance through regular monitoring, periodic assessments, and ongoing employee training programs to foster a culture of privacy.



Phase I: Establish a Privacy Blueprint

Establishing a strong privacy blueprint is the foundation of an effective privacy program. It involves defining the organization's strategic privacy direction, governance framework, and securing executive commitment to drive privacy initiatives forward.





Phase II: Assess Current Practices

Building on the foundation set in Phase I, this phase focuses on identifying personal data practices, determining critical business units that require increased supervision, and assessing the organization's current regulatory compliance posture. The insights gained help in developing a structured roadmap that will be operationalized in Phase III.

Personal Data Inventorization

- Identify and document the types of personal data processed across the organization.
- Map data flows to understand where data resides and how it is shared internally and externally.
- Maintain an up-to-date Record of Processing Activities (RoPA) to enhance transparency and accountability.

Current State Assessment

- Evaluate existing privacy policies, procedures, and controls against applicable PDPPL requirements
- Assess the effectiveness of implemented privacy measures and organizational readiness.
- Identify gaps in compliance and potential risks associated with data processing activities.

Roadmap Development

- Develop an implementation roadmap strategic plan to address identified gaps and align privacy efforts with business objectives.
- Define key milestones, timelines, and responsibilities for implementing necessary improvements.
- Prioritize actions based on regulatory obligations and business priorities.



Phase III: Implement Privacy Requirements (1/2)

Building on the regulatory requirements and the way forward identified in Phase II, Phase III focuses on translating these requirements into actionable measures to establish a fully operational privacy program.

Privacy Policies and Procedures

- Develop an overarching Privacy policy encompassing applicable regulatory requirements.
- Develop supporting procedures on how to operationalize the various applicable regulatory requirements.
- Obtain top-management buy-in and socialize the developed documents.

Personal Data Lifecycle Management

- Implement a structured approach for managing personal data from collection to disposal.
- Ensure data minimization, data quality, storage limitation and data security across lifecycle.
- Define retention schedules based on legal and business requirements.

Notice and Consent Management

- Develop and present privacy notices at data collection points.
- Obtain valid and informed consent from individuals before processing their data, with proper mechanisms for withdrawal.

Third Party and Cross Border Management

- Maintain records of Data Processors and Cross Border Data Transfers
- Safeguard data disclosures to Third Parties via Data Processing Agreements
- Ensure all risks associated with cross border data transfers are managed with appropriate mitigation measures



Phase III: Implement Privacy Requirements (2/2)

Building on the regulatory requirements and the way forward identified in Phase II, Phase III focuses on translating these requirements into actionable measures to establish a fully operational privacy program.

Individual Rights Management

- Implement mechanisms to facilitate the exercise of data subject rights such as access, correction, erasure, and consent withdrawal.
- Verify individuals' identities before processing rights requests and provide timely responses.
- Communicate reasons for any refusal (if applicable).

Personal Data Breach Management

- Develop an incident response plan to manage data breaches effectively.
- Ensure data breach notification requirements are adhered to as per PDPPL requirements.
- Identify lessons learned and implement mitigation measures to prevent similar incidents from recurring.

Implement Privacy by Design

- Embed privacy principles into business processes and technology solutions from the outset.
- Conduct Data Privacy Impact Assessments (DPIAs) to identify and mitigate risks.
- Ensure privacy considerations are integrated into product development lifecycles.

Special Nature Data Processing

- Identify and obtain necessary approvals for processing special categories of personal data.
- Implement enhanced security measures such as encryption and access controls.
- Regularly review such data processing activities to ensure compliance.



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Phase IV: Sustain and Improve Compliance

This phase ensures that privacy measures remain effective, aligned with evolving regulatory requirements, and ingrained into the organization's operational framework.

Continuous Monitoring and Improvement

- Conduct periodic reviews of privacy practices to identify enhancement opportunities and maintain compliance.
- Stay informed about legislative changes and industry best practices to ensure ongoing regulatory alignment.
- Integrate feedback from employees, customers, and regulators to refine privacy practices and address emerging risks.
- Conduct regular audits and assessments to evaluate the effectiveness of privacy controls and identify any weakness.

Employee Training and Awareness Program

- Educate employees on the key elements of the Personal Data Privacy Protection Law (PDPPL) and their responsibilities.
- Provide role-based training to ensure specific privacy practices are understood and followed at all organizational levels.
- Offer ongoing refresher sessions to keep employees updated on evolving privacy requirements and emerging risks.
- Ensure new employees are made aware of organizational privacy practices as part of their onboarding trainings.



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

Thank You