State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

Individuals' Complaints

PDPPL-02050214E

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-02050205E	Individuals' Rights Guidelines for Regulated Entities (English)
PDPPL-02050217E	Personal Data Breach Notifications 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 "Individuals' Complaints 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 Personal Data Privacy Protection Law (PDPPL) requires controllers to put in place a system to handle complaints from individuals regarding their personal data and / or privacy under Article 11.
- The PDPPL also enables individuals to complain to the National Cyber Governance and Assurance Affairs about a controller and the National Cyber Governance and Assurance Affairs under Article 26.
- Complaints to the controller and / or the National Cyber Governance and Assurance Affairs may be in relation to any provisions of the PDPPL or related ministerial decisions.
- The National Cyber Governance and Assurance Affairs may issue a reasoned binding decision requiring the controller to take action following an investigation.
- The controller may raise a grievance against a decision issued by the National Cyber Governance and Assurance Affairs within 60 days of its issue.
- The National Cyber Security Agency may issue a decision on any grievance raised by a controller within 60 days. If the Minister does not do so the controller should consider this a rejection of the grievance and comply with the reasoned binding decision in full.

2. Introduction

The PDPPL requires controllers receive and investigate complaints from individuals about how their personal data is processed. It also requires the National Cyber Governance and Assurance Affairs to investigate complaints about controllers from individuals and issue reasoned binding decisions compelling the controller to take action where the National Cyber Governance and Assurance Affairs sees fit following any investigation.

These guidelines set out the obligations of controllers regarding individuals' complaints in more detail and how the National Cyber Governance and Assurance Affairs may behave when investigating them.

3. What does the PDPPL say about complaints?

3.1. Complaints to Controllers

Article 11 (4) of the PDPPL says:

> *"The Controller shall: Develop an internal system to **receive and look into complaints**, data access requests and omission/correction requests; and shall provide access thereto to Individuals."*

Controllers must establish a procedure to enable individuals to make a complaint to the controller in relation to their personal data or their privacy. This complaints procedure should enable the recording and tracking of complaints and a process to be followed when they are made verbally. Controllers may wish to implement an IT system to manage their complaints procedure, the size and scope of this system will depend on what is appropriate for the size and complexity of the controller's organisation.

Controllers must take all reasonable steps to achieve an agreed resolution to the complaint to the satisfaction of the individual or respond with reasons why they do not believe any action is necessary on their part.

For further information on procedures for managing complaints, please refer to the "General guidelines on dealing with requests" section of the Individuals' Rights Guidelines for Regulated Entities.

3.2. Complaints to the National Cyber Governance and Assurance Affairs

Article 26 of the PDPPL says:

> *"An Individual may file a **complaint to the Competent Department** in case of **violating provisions hereof and the issued decisions** in the implementation thereof.*
>
> *The Competent Department may, after investigating received complaints and proving the seriousness thereof, **issue a reasoned decision binding the Controller or Processor**, as the case may be, to rectify such breach within a period it specifies.*
>
> *The **Controller or Processor may raise a grievance** against such decision to the Minister, **within sixty days** from the notification date thereof.*
>
> ***The Minister shall decide on the grievance within sixty days** from the date of the submission thereof, and the lapse of such period without a response shall be considered as an implicit rejection of the grievance, and the decision of the Minister thereon shall be final."*

An individual may file a complaint to the National Cyber Governance and Assurance Affairs in any case where they believe a Controller has processed personal data in a way that is not compliant with the PDPPL or any related ministerial decisions. This could include, but is not limited to:

- contravening the principles of processing;
- not complying with an individual's complaint or request regarding their rights; or
- not keeping personal data secure.

The National Cyber Governance and Assurance Affairs may investigate any complaints lodged by individuals and, following an investigation, issue a binding decision setting actions that a Controller must take to rectify any breach found within a period deemed appropriate to the risk posed by any violation.

The Controller or Processor may raise a grievance against a decision to the Minister, within sixty days of the decision being made. The Minister will either make a final decision within 60 days of the grievance being raised or not respond which will be considered a rejection of such grievance.

4. What may individuals make a complaint about?

Where an individual is unhappy about the manner in which the controller has handled their personal data, they have a right to raise a concern with the National Cyber Governance and Assurance Affairs.

Article 26 of the PDPPL says:

> *"An Individual may file a **complaint to the Competent Department** in case of **violating provisions hereof and the issued decisions** in the implementation thereof.*

This means that individuals can file a complaint to the National Cyber Governance and Assurance Affairs relating to any provision of the PDPPL or any related ministerial decisions. Complaints which are made directly to controllers under Article 11(4) may also be made in relation to any provision of the PDPPL or related ministerial decisions.

Examples of issues such complaints may cover are:

- concerns about a controller's response to a request the individual has made to access copies of their personal data or make incorrect data correct;
- concerns about their personal data being breached by an organisation, or;
- any other concerns about how a controller is handling the individual's personal data in any way, for example not complying with the principles of data privacy.

The examples above are not exhaustive.

Controllers are accountable for their compliance with the PDPPL and related Ministerial Decisions. For copies of these documents, please refer to the PDPPL section of the National Cyber Governance and Assurance Affairs website.

5. How will the National Cyber Governance and Assurance Affairs manage complaints it receives?

5.1. Assess scope and validity

When an individual file a complaint with the National Cyber Governance and Assurance Affairs, the National Cyber Governance and Assurance Affairs will review the complaint to confirm that it is related to the PDPPL and falls within the National Cyber Governance and Assurance Affairs remit to address. The National Cyber Governance and Assurance Affairs may request further information or evidence from the individual to support their complaint.

Once satisfied that the complaint raised is related to the PDPPL or any related ministerial decisions, the case will be progressed as appropriate. If the case does not fall within the remit of the National Cyber Governance and Assurance Affairs under the PDPPL then the individual will be informed of this and the complaint will be dismissed.

5.2. Facilitate an agreed resolution

In the first instance, the National Cyber Governance and Assurance Affairs will seek to arrange an agreed resolution to the complaint between the individual and the controller where there is a reasonable likelihood of this being achieved in a reasonable timeframe.

Where it appears that the complaint has a valid basis and may involve a breach of the PDPPL, the National Cyber Governance and Assurance Affairs may encourage the controller to rectify any issues identified voluntarily and consider making an appropriate gesture to resolve the complaint.

5.3. Taking actions to resolve the complaint without investigation

Where an agreed resolution is not achievable (for example where the individual does not accept a gesture on the part of your controller), the National Cyber Governance and Assurance Affairs may take various steps to resolve the matter before opening an investigation. These include but are not limited to:

- dismissal of the complaint;
- providing advice to a controller in relation to the matter;
- requesting that a controller take action to rectify the situation.

5.4. Undertaking a full investigation

Where the actions taken by the National Cyber Governance and Assurance Affairs do not result in a dismissal of the complaint or the controller taking appropriate action to rectify the situation, the National Cyber Governance and Assurance Affairs may undertake an investigation.

Generally speaking, the National Cyber Governance and Assurance Affairs will only consider commencing an investigation where the matter raised indicates that the alleged data breach is of an extremely serious nature and/or indicative of a systemic failing within the controller in question.

During its investigation the National Cyber Governance and Assurance Affairs may request further information from the individual and / or the controller. The National

Cyber Governance and Assurance Affairs recommends that controllers provide any information requested voluntarily during an investigation.

Article 29 of the PDPPL says:

> *The Ministry employees, **authorised as law enforcement officers** as per a decision by the Public Prosecutor, in agreement with the Minister, **may detect and prove crimes committed** in violation of provisions hereof.*

Employees of the National Cyber Governance and Assurance Affairs who are authorised as law enforcement officers may use relevant powers, allowed for in Article 29 and conferred by ministerial decision, to gather information and investigate complaints where they see fit.

At any point during the investigation, the National Cyber Governance and Assurance Affairs may resolve the complaint through agreement between the individual and the controller or through the controller agreeing to rectify the situation.

5.5. Issuing a reasoned decision

Article 26 (2) of the PDPPL says:

> *"The Competent Department may, after investigating received complaints and proving the seriousness thereof, **issue a reasoned decision binding the Controller or Processor**, as the case may be, to rectify such breach within a period it specifies."*

After investigating a complaint from an individual, the National Cyber Governance and Assurance Affairs may issue a binding reasoned decision requiring the controller to rectify any confirmed breach within a specific period of time determined by the National Cyber Governance and Assurance Affairs. This could, for example, compel the controller to comply with an individual's request regarding their rights, require the controller to notify individuals of a breach or require the controller to implement specific action to comply with the PDPPL.

6. What happens after a complaint is resolved or the National Cyber Governance and Assurance Affairs has issued a reasoned decision?

6.1. Controller raising a grievance

Article 26 (3) of the PDPPL says:

> *"The **Controller or Processor may raise a grievance** against [a binding reasoned decision] to the Minister, **within sixty days** from the notification date thereof."*

If the controller does not agree with the binding reasoned decision issued by the National Cyber Governance and Assurance Affairs they may raise a grievance against the decision within 60 days of the notification date of the decision.

6.2. Ministerial adjudication on grievance

Article 26 (4) of the PDPPL says:

> *"**The Minister shall decide on the grievance within sixty days** from the date of the submission thereof, and the lapse of such period without a response shall be considered as an implicit rejection of the grievance, and the decision of the Minister thereon shall be final."*

The Minister may issue a decision on the grievance raised by the controller within 60 days of its submission. If no response is received from the Minister the controller must comply with the binding reasoned decision issued by the National Cyber Governance and Assurance Affairs in full or risk being found in breach of the law and subject to enforcement action.

For further information on breaches of the PDPPL, please refer to the Personal Data Breach Notifications Guidelines for Regulated Entities.

End of Document