State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

Individuals' Complaints

PDPPL-02050220E

Guidelines for Individuals

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-02050219E	Individuals' Rights Guidelines for Individuals (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 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.

Individuals may make complaints to the controller and / or the National cyber governance and assurance affairs 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

Article 3 of the PDPPL provides individuals with the right to the protection and the lawful processing of their personal data. This means that individuals can expect their personal data to be processed in accordance with the PDPPL.

If individuals believe that their personal data is not being protected or processed lawfully, the PDPPL requires controllers to enable individuals to make complaints to them about how their personal data is being processed. Controllers must investigate complaints from individuals and rectify any practices that are found, upon investigation, to not be compliant with the PDPPL.

The PDPPL also enables individuals to make complaints to the National cyber governance and assurance affairs about the processing practices of any organisation where the individual believes that their personal data is not being processed in accordance with the PDPPL. The National cyber governance and assurance affairs is required 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 how individuals should make complaints to controllers and the National cyber governance and assurance affairs and how the National cyber governance and assurance affairs may behave when investigating them. The requirements regarding the complaints of individuals can be found in Articles 11 (4) and 26 of the PDPPL and are explained in more detail below.

3. What does the PDPPL say about complaints?

3.1. Complaints to Controllers

Article 11 (4) of the PDPPL says:

"Develop and implement an internal system to **receive and investigate complaints**, data access requests and omission/correction requests; and shall provide access thereto to Individuals."

Individuals must be able to make complaints to controllers directly through a procedure that controllers are required to set up to receive and look into complaints in relation to their personal data or their privacy.

Controllers should inform Individuals of how to make complaints when collecting their personal data. Individuals should be able to find information on how to make complaints about the way a controller processes their personal data easily, for example through their website privacy notice.

Controllers must take all reasonable steps to achieve an amicable 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.

Individuals should exhaust all opportunities to complain and reach a satisfactory resolution with the controller before making a complaint to the National cyber governance and assurance affairs.

For further information on the rights that are afforded to individuals by the PDPPL, please refer to the Individuals' Rights Guidelines for Individuals.

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 file a complaint 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.

This means that individuals can file a complaint relating to any potential violation of the PDPPL or any related ministerial decisions regarding its implementation. This also applies to any complaints made directly to controllers under the procedure provided for under Article 11 (4).

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.

For more detailed information on what individuals may wish to complain about, please refer to Appendix A - Information on what individuals may wish to complaint about.

For information on what controllers must do to comply with obligations under the PDPPL, please refer to the National cyber governance and assurance affairs PDPPL Guidance Hub for guidelines and information on how to comply.

5: How should individuals make a complaint?

When making a complaint to a controller, individuals may contact the controller through any channel. Individuals should, however, use the channel provided by the controller specifically for making complaints regarding personal data. This may be, for example, through an online form or through contact with a specific email address. Information on how to complain to a controller should be provided in the controller's privacy notice.

The various information individuals should include when making a complaint are:

- The reason for the complaint.
- Any information that can enable the controller to identify their records of the individual such as an account number.
- A clear and concise summary of the concerns being raised.
- Information on the impact that the subject matter of the complaint has had on the individual including any damage to the individual's privacy or personal data.
- When making a complaint, individuals should:
- Raise the complaint with the controller as soon as possible after the issue arises or event occurs that is being complained about.
- Send the complaint to the address that the controller specifies to ensure that it gets to the responsible department as quickly as possible.
- Write the complaint in clear and plain language so that the complaint may be easily understood.
- Provide specific information relating to the event or issue that is being complained about and do not include matters unrelated to the complaint about data privacy.
- Provide all available information at the time of making the initial complaint including copies of any evidence. Do not raise multiple unrelated complaints at once as part of the same submission. If the controller responds and the individual thinks that the controller has not understood the complaint or given a complete response, the individual should inform the controller and provide clarification, if possible.
- Request and respect timescales. Individuals should ask when they can expect the controller to respond and resist any temptation to contact them again before that. If the individual does not receive a response within 30 calendar days, however, they could follow up with the controller.
- Keep a record of dates and times that communications were made and copies of any communications including any documentation provided.

For a template letter that individuals may wish to use to make a complaint to a controller, please refer to Appendix B - Template letter for making a complaint to a controller.

Individuals should exhaust the controller's complaints process prior to raising a complaint with the National cyber governance and assurance affairs. It is likely that if this has not been done, the National cyber governance and assurance affairs will direct individuals to raise a complaint with the controller before proceeding with the National cyber governance and assurance affairs complaints process.

5.1. When should I raise my complaint to the National cyber governance and assurance affairs?

After exhausting the complaints procedure of a controller, individuals may feel that the controller has been uncooperative, not sufficiently dealt with their complaint or is wilfully not complying with their obligations under the PDPPL or related ministerial decisions.

Individuals may raise a complaint with the National cyber governance and assurance affairs about any violation of the PDPPL where they are not satisfied with the response or proposed remedy of a controller to an issue raised with them by the individual.

To raise a complaint with the National cyber governance and assurance affairs individuals should refer to the complaints page on the PDPPL section of the National cyber governance and assurance affairs website to submit a complaint. Individuals should include copies of their original complaint, any supporting documentation provided and copies of their interaction with the controller regarding the complaint and related resolution that they are not satisfied with.

6. How will the National cyber governance and assurance affairs manage complaints it receives?

6.1. Assess scope and validity

When an individual files 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.

6.2. 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.

6.3. 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.

6.4. 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.

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.

6.5. 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.

7. What happens after a complaint is resolved or the National cyber governance and assurance affairs has issued a reasoned decision?

7.1. 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.

7.2. 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.

Appendix A - Information on what individuals may wish to complaint about

Individuals have the right to be confident that organisations protect their personal data and process it lawfully and in line with good practice.

Cases where individuals may feel that a controller has failed to meet the standards of processing required by the PDPPL may fall into a number of categories. Areas that individuals complaints may relate to are set out below.

Contravening the principles of processing

Examples of complaints about the principles of processing are:

- **transparency, honesty and respect for human dignity:** "the controller did not clearly inform me of how they were going to process my personal data. I gave them my information to open an account. They do not have a public privacy notice and I never received any information on how they would use my data and what their permitted reason for doing so was."
- **data minimisation:** "I wanted to enter a prize draw and, on top of requesting my name, contact details and account number, asked for my blood type and national ID number which was not necessary to enter me into the draw."
- **accuracy:** "I provided personal health data about my dietary requirements and then was provided with food that I had not requested because the incorrect requirements had been stored by the controller."
- **storage limitation:** "I provided my personal data to make a reservation three years ago and recently began receiving requests from the controller to provide information on my preferences. The controller should not have kept my personal data for three years when they only needed it to organise my booking."
- **integrity and confidentiality:** "Ever since I provided my phone number to book a table for dinner at a hotel the controller operates, I have received numerous messages trying to sell products and services to me that are unrelated. I believe the controller did not keep my personal data confidential."
- **purpose limitation:** "I provided my contact details so that a controller could contact me about a specific gym membership, since then the controller has been sending me information about unrelated products that they sell."
- **accountability:** "a controller that I provided my personal data to shared it with a processor to provide me with the credit card I had ordered, the processor has since tried to sell me other products and the controller has told me that they are not accountable for the actions of the processor."

Not complying with an individual's complaint or request regarding their rights

Examples of complaints about their PDPPL rights:

- **the right to protection and lawful processing:** "I believe the controller does not process my personal data under a permitted reason, they have not asked me for consent and they cannot inform me of why they process my data.
- **the right to withdraw consent:** "I consented to the controller sending me marketing emails about their products and no longer wish to receive such marketing. I contacted the controller to withdraw my consent and inform them that I no longer wished to receive such emails. They have told me that I have given consent and now cannot change my mind."

- **the right to object to processing in certain circumstances:** "I provided my personal data to a controller to subscribe to an online service of theirs. They have since changed how they process my data, conducting analytics on my preferences, and I believe this is not necessary to continue providing me with the service. I objected to them analysing my data in this way and the controller has continued to do so."
- **the right to erasure:** "I informed a controller that since I was no longer a member of their loyalty scheme I wanted them to delete my personal data that they held. They refused to do so."
- **the right to request correction:** "We have a family account with a controller and they have another person linked to it who is not a family member. We have asked them to correct this and remove the person from our account but this has not been done."
- **the right to be notified of processing:** "I asked a controller to provide specific information on how they are processing my personal data but they refused."
- **the right to be notified of inaccurate disclosure:** "I applied for a loan and a controller disclosed to the company that I had applied with that I already had 3 credit cards. This was incorrect as I had closed all three cards but was the reason I had my loan application rejected. I asked the disclosing controller to provide evidence that the disclosure they had made was incorrect to the loan provider so that I could reapply and they refused to do so".
- **the right to access their personal data:** "I asked a controller to provide me with a copy of the data I had provided to them. They refused to do so."

Not keeping personal data secure

Examples of complaints data security are:

data security: "a controller processing my personal data did not keep it secure and my personal data has now been compromised and is being used by other organisations."

Appendix B - Template letter for making a complaint to a controller

[Your full address]

[Phone number]

[The date]

[Name and address of the organisation you are addressing]

[Reference number (if this has been provided with an initial response)]

Dear [Sir or Madam / name of the person you have been in contact with prior to this communication]

Subject: Complaint under the PDPPL regarding my personal data

[Provide your full name and address along with any other details such as account number that may help identify you]

I am concerned that you have not handled my personal data properly in accordance with the Personal Data Privacy Protection Law (PDPPL).

[Provide details of your concern, explaining clearly and simply what has happened and, where appropriate, the impact that it has had on you.]

I understand that before reporting my concern to the Compliance and Data Protection (National cyber governance and assurance affairs) Department, I should give you the opportunity to resolve the issues raised in my complaint.

Please send a full response within 30 days. If you cannot respond within that time frame, please notify me accordingly of when you will be able to respond to the complaint.

If there is anything you would like to discuss, please contact me using the following details [email is advised in order to ensure communications are maintained].

Yours faithfully,

[Signature]

End of Document