State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

Individuals' Rights

PDPPL-02050219E

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-02050204E	Permitted Reasons Guidelines for Regulated Entities (English)
PDPPL-02050220E	Individuals' Complaints Guidelines for Individuals (English)
PDPPL-02050213E	Privacy Notice 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' Rights Guidelines for Individuals".

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

- Personal data is information about an individual through which that individual could be identified, either through that personal data or when that personal data is combined with any other data.
- It is important that personal data is only used in ways that individuals would reasonably expect, and that it stays safe. The Personal Data Privacy Protection Law (PDPPL) is in place to ensure that personal data is processed legally, kept secure and not used in a way that causes damage to individuals.
- The PDPPL provides individuals with a number of rights in relation to their personal data. These rights help ensure that everyone's data is used properly and legally.
- These rights are as follows:
    - the right to protection and lawful processing;
    - the right to withdraw consent;
    - the right to object to processing in certain circumstances;
    - the right to erasure;
    - the right to request correction;
    - the right to be notified of processing;
    - the right to be notified of inaccurate disclosure; and
    - the right to access their personal data.
- Some of these rights are always available, whereas some are only available in certain circumstances.
- These guidelines will set out more detail about each of these rights, including when and how individuals can exercise them.
- These guidelines should be read in conjunction with the PDPPL, related ministerial decrees, and other guidelines issued by the National Cyber Governance and Assurance Affairs.

2. Introduction

Chapter 2, Articles 3, 4, 5, 6 and 7 of the PDPPL on individuals' rights and Chapter 3, Article 9 of the PDPPL on Controller and Processor Obligations set out certain rights that individuals have with respect to their personal data. These are as follows:

- the right to protection and lawful processing;
- the right to withdraw consent;
- the right to object to processing in certain circumstances;
- the right to erasure;
- the right to request correction;
- the right to be notified of processing;
- the right to be notified of inaccurate disclosure; and
- the right to access their personal data.

Some of these rights apply in all circumstances and others apply only in certain circumstances. These circumstances are explained further below. Controllers must understand the conditions for the application of each right so they can carry out their obligations accordingly.

Controllers must enable individuals to exercise these rights if they process their personal data, or if another controller or processor processes their personal data on their behalf (e.g. a processor).

These guidelines set out each right in more detail and have been developed to help individuals understand when and how they can exercise them.

The information in these guidelines is not exhaustive and should be read in conjunction with the PDPPL, related ministerial decrees, and other guidelines issued by the National Cyber Governance and Assurance Affairs.

3. The rights in brief

3.1. Why is the permitted reason for processing important?

The first principle requires that controllers process all personal data within the bounds of transparency, honesty and respect for human dignity. If no permitted reason applies to the controller's processing, their processing will be unlawful and in breach of the principle of honesty.

The permitted reason for the controller's processing can also affect which rights are available to individuals as set out below:

Permitted reasons where rights apply	Individual Rights						
	Withdraw consent	Object	Erasure	Request correction	Inaccurate disclosure	To be notified	To access / obtain copy
Consent	X	X	X	X	X	X	X
	-	By virtue of the right to withdraw consent	By virtue of the right to withdraw consent	Supporting evidence required	Supporting evidence required	-	-
Contract				X	X	X	X
				Supporting evidence required	Supporting evidence required	-	-
Legal obligation				X	X	X	X
		-	-	Supporting evidence required	Supporting evidence required	-	-
Legitimate interest		X	X	X	X	X	X
		-	-	Supporting evidence required	Supporting evidence required	-	-

The individual's right to be notified under Article 6 and requirements under Article 9 mean that controllers must provide people with information about their permitted reasons for processing. This means controllers need to include these details in their privacy notice.

3.2. In which circumstances do the rights apply?

Some rights apply in all circumstances and others apply only in certain circumstances. Controllers must understand the conditions for the application of each right so they can carry out their responsibilities accordingly.

Controllers must enable individuals to exercise these rights if they process their personal data, or if another controller or processor processes their personal data on their behalf (e.g. a processor).

Circumstances in which the rights apply	Individual Rights						
	Withdraw consent	Object	Erasure	Request correction	Inaccurate disclosure	To be notified	To access
In any case	X			X	X	X	X
Where processing is no longer necessary		X	X	X	X	X	X
Where processing is beyond the extent required		X	X	X	X	X	X
Where processing is discriminatory		X	X	X	X	X	X
Where processing is unfair		X	X	X	X	X	X
Where processing is Illegal		X	X	X	X	X	X
Upon cessation of purpose for processing			X	X	X	X	X
Justification for storing expires			X	X	X	X	X

These guidelines set out each right in more detail below and supports controllers in understanding their obligations regarding these rights. It also sets out the actions controllers should take to prepare to deal with requests from individuals.

4. The rights in more detail

4.1. The right to protection and lawful processing

Article 3 of the PDPPL says:

> *"Each Individual has the **right to the protection of the Personal Data** thereof that shall be processed only within the framework of transparency, honesty, and respect of human dignity, and acceptable practices **according to provisions hereof.**"*

What does the right to protection and lawful processing mean in practice?

Controllers are under a duty to protect individuals' personal data and ensure that they process their personal data lawfully.

To properly protect individuals' personal data, controllers must:

- Process it in accordance with the provisions and principles of the PDPPL;
- Ensuring that the data is kept securely, so that it is not accessible, intentionally or inadvertently, to any person or organisation that it shouldn't be;
- Providing individuals with control over their personal data by enabling them to exercise their rights under the PDPPL.

To lawfully process individuals' personal data, controllers must:

- Processing the personal data in accordance with the PDPPL, which includes having either a Lawful Purpose for processing, explicit written consent to process the data, or having a valid exemption that applies to the processing in question.

If individuals are concerned about the manner in which a controller is handling their personal data, they are entitled to complain to the organisation about this. They are also entitled to raise a concern to the National Cyber Governance and Assurance Affairs if they are not satisfied with the outcome of their complaint to a controller.

Further information

For more information on lawful processing, please refer to the Guidelines on Permitted Reasons for Processing for Regulated Entities.

For more information on how to make a complaint to a controller or the National Cyber Governance and Assurance Affairs please refer to the Guidelines on Complaints for Individuals.

4.2. The right to withdraw consent

Article 5.1 of the PDPPL says:

> "*An Individual may at any time:* **Withdraw** the prior **consent** thereof for Personal Data Processing.''

What does the right to withdraw consent mean in practice?

Where controllers are relying on an individual's explicit written consent to process their personal data, the individual has the right to withdraw this consent. This means that:

- individuals may withdraw their previously given consent at any time;
- controllers must act on individuals' requests as soon as possible;
- controllers must provide individuals with information on how they can withdraw their consent and should not make it difficult for them to do so;
- if individuals choose to withdraw their consent, controllers must stop processing their personal data; and
- individuals must not be penalised for withdrawing their consent.

Further information

For further information on consent please refer to the Guidelines on Permitted Reasons for Processing for Regulated Entities.

4.3. The right to object

Article 5.2 of the PDPPL says:

> *''An Individual may at any time: **Object** to processing the personal data thereof if such processing is not necessary to achieve the purposes for which such personal data have been collected or where such collected personal data are beyond the extent required, discriminatory, unfair and/ or illegal.''*

This provides individuals with the right to object to the processing of their personal data.

Individuals may make requests in relation to some or all of the personal data controllers hold on them, or data that controllers are processing about them for a specific purpose.

What does the right to object mean in practice?

An individual may exercise the right to object in certain circumstances. Where such circumstances apply, individuals can stop or prevent a controller from using their personal data. These circumstances are set out below.

Under what circumstances does the right to object apply?

The right to object applies in the following circumstances:

- When the processing of an individual's personal data is not necessary to achieve the purposes for which it was originally collected;
- When decisions are made about an individual based solely on the automated processing of their personal data and this processing leads to discriminatory outcomes.
- Where a controller is processing an individual's personal data:
    - Beyond the extent required;
    - In a way that is discriminatory;
    - Unfair; and/or
    - Illegal.

For more information on what these terms mean in practice, please refer to the section on key words and phrases below.

In what ways can individuals exercise their right to object?

Individuals can object to either the processing of all the personal data a controller is processing about them or to just some of the personal data they are processing. for a specific purpose.

Individuals must provide a specific purpose for objecting to processing. Individuals must explain to the controller why they believe the controller should stop processing their data in such a way.

Individuals can make their request either verbally or in writing. The National Cyber Governance and Assurance Affairs recommends that, where a request is made

verbally, individuals follow it up in writing to ensure that they have evidence of making the request for their records.

How should controllers respond to a request to exercise the right to object?

- The controller should tell the individual about whether they will enable the individual to object and carry out the request to stop the processing or not.
- If the controller accepts the request to exercise the right to object, the controller must stop processing the individual's personal data for the specific purpose identified in the request. The controller may, however, be able to continue using the individual's personal data for purposes other than those referred to in the request.
- If a controller concludes that they have a valid reason to continue processing in spite of the request it should explain its decision and rationale to the individual and provide proof of a strong reason that overrides the individual's objection. It should also inform the individual of their right to complain to the controller and to the National Cyber Governance and Assurance Affairs.
- A controller may refuse to comply with an individual's request if the request is excessive or malicious or if an exemption applies.
- When individuals object to their personal data being used to make decisions about them based solely on automated processing which leads to discriminatory outcomes, a controller may also take steps to:
    - Ensure there is human intervention in the process; and
    - Ensure a competent person analyses the decisions made to make sure they are not discriminatory, and change the outcome if appropriate.

Further information

For more information on what 'excessive or malicious' means in practice, please refer to the section on key words and phrases below.

For more information on how to make a complaint to a controller or the National Cyber Governance and Assurance Affairs please refer to the Guidelines on Complaints for Individuals.

4.4. The right to erasure

Article 5.3 of the PDPPL says:

> *''An Individual may at any time: Request **omission or erasing** of the personal data thereof in any of the cases provided above (1 and 2), upon cessation of the Purpose for which the processing was conducted, or where all justifications of storing such personal data by the Controller cease to exist.''*

What does the right to erasure mean in practice?

The right to erasure, also known as the 'right to be forgotten', means individuals have the right to request that a controller delete any personal data of theirs that holds. In some circumstances, they must then do so.

Under what circumstances does the right to erasure apply?

The right to erasure only applies in the following circumstances:

- *When an individual withdraws their consent*

Where the controller is relying on an individuals consent as the permitted reason for processing, and the individual withdraws this consent.

- *When the processing is no longer necessary*

When the processing of the individual's personal data is no longer necessary to achieve the purpose for which the controller collected it.

- *When the personal data collected is beyond the extent required*

When the controller has collected more than the minimum amount of personal data required to fulfil their purpose for processing.

- *When the processing of the personal data is discriminatory, unfair, or illegal*

Discriminatory: The processing of personal data will be discriminatory if such processing leads to the individual being treated unfairly, and receiving different, and often worse treatment, than other individuals or groups.

Unfair: The processing of personal data will be unfair if it is unduly detrimental, unexpected or misleading. Controllers should only handle personal data in ways that the individual would reasonably expect and should not use it in ways that have unjustified adverse effects on the individual.

Illegal: The processing of personal data will be illegal if it is not compliant with the PDPPL, or with any other law in the State of Qatar.

- *When the purpose for processing no longer exists*

When the purpose for processing the personal data ceases to exist.

- *Where the reasons for storing the personal data no longer exist*

When the reason/s for retaining the personal data cease to exist.

In what ways can individuals exercise their right to erasure?

Individuals can request for the erasure of any or all of their personal data held by a controller or processed on their behalf.

Individuals must also specify which personal data they would like the controller to delete. They must also provide a specific purpose for erasure and explain why they believe the controller should erase the personal data referred to in the request.

Individuals can make their request either verbally or in writing. The National Cyber Governance and Assurance Affairs recommends that, where a request is made verbally, individuals follow it up in writing to ensure that they have evidence of making the request for their records.

How should a controller respond to a request to exercise the right to erasure?

- The controller should tell the individual about whether they will carry out the individual's request for the controller to erase the individual's personal data or not.
- If a controller concludes that they have a valid reason to continue processing in spite of the request it should explain its decision and rationale to the individual and provide proof of a strong reason that overrides the individual's objection. It should also inform the individual of their right to complain to the controller and to the National Cyber Governance and Assurance Affairs.
- A controller may refuse to comply with an individual's request if the request is excessive or malicious or if an exemption applies.
- If the controller accepts the request to exercise the right to erasure, the controller must erase the personal data specified in the request.
- The controller should inform anyone else they have shared the individual's data with about the erasure, unless this involves a disproportionate effort or is impossible.
- If the individual's data has been made public online – such as on social networks, forums or websites – then the controller must take reasonable steps to inform the people with responsibility for these sites to erase links or copies of that data.

Further information

For more information on what 'excessive or malicious' means in practice, please refer to the section on key words and phrases below.

For more information on how to make a complaint to a controller or the National Cyber Governance and Assurance Affairs please refer to the Guidelines on Complaints for Individuals.

4.5. The right to request correction

Article 5.4 of the PDPPL says:

> *''An Individual may at any time: Request **corrections** to the personal data thereof. A request so made shall be accompanied with proof of the accuracy of such request.''*

What does the right to request correction mean in practice?

Individuals have the right to challenge the accuracy of personal data held about them by a controller, and ask for it to be corrected or deleted. If personal data is incomplete, an individual can ask the organisation to complete it by adding the additional required information under any circumstances.

To exercise this right individuals must provide proof of the inaccuracies that they are challenging. Details on how individuals should provide this evidence are set out below.

How can individuals exercise their right to request correction?

Individuals should contact the controller and inform them that they are challenging the accuracy of personal data and that they want it to be corrected. Individuals should:

- tell the controller clearly what they believe is inaccurate or incomplete;
- explain to them how the controller should correct it; and
- provide evidence of the inaccuracies

Individuals can make a request for the correction of their personal data either verbally or in writing. The National Cyber Governance and Assurance Affairs recommends that, where a request is made verbally, individuals follow it up in writing to ensure that they have evidence of making the request for their records.

How can Individuals provide evidence of inaccuracies?

Individuals must provide the controller with evidence that the personal data they hold about them is inaccurate.

Individuals may provide evidence by:

- *Providing proof of the correct personal data*

  Individuals should demonstrate the inaccuracy by showing the controller some documentary evidence which includes the correct personal data.

  For example, if a controller had an incorrect record of the individual's date of birth, the individual could prove this is incorrect by showing them an official ID document containing the correct date.

- *Providing proof that the personal data is incomplete*

  Individuals should show the controller evidence which proves that the personal data they hold on them is incomplete.

  This could be in the form of any kind of documentary evidence which shows the personal data that they are missing from their records.

Can personal data that records a mistake or an opinion be corrected?

If data refers to a mistake that was made that was later corrected:

- The fact the mistake was made is a statement of fact, and therefore keeping a record of the fact that it happened and has been corrected is permissible. A controller may therefore refuse to change the personal data that was incorrect in these circumstances as this would be held for record keeping purposes to demonstrate a correction was made.

If data refers to an opinion:

- The controller should make it clear within the record that the data recorded is an opinion and, where appropriate, whose opinion it is. If the controller does this the record of the opinion will be accurate and the controller will not need to correct or delete the record.

How should a controller respond to an individual's request for correction?

Upon receiving a request for correction and supporting evidence, the controller should take reasonable steps to investigate whether the data is accurate. As a part of these reasonable steps they should:

- consider the individuals arguments; and
- consider the evidence of the inaccuracy they have provided.

The controller should also be able to demonstrate that they have carried out this investigation and have considered the individual's arguments and evidence.

Once this investigation has been completed, the controller should contact the individual and confirm either:

- that the data has been corrected, deleted or added to; or
- that it is rejecting the request and therefore will not make the requested change(s) to the data.

If the controller agrees that a correction is required, they should inform anyone else they have shared the personal data with about the correction so that those third parties can correct their records too unless this involves a disproportionate effort or is impossible.

If the controller decides that correction is not necessary, the controller should explain to the individual why they believe the data is accurate in its present form.

A controller may refuse to comply with an individual's request if the request is excessive or malicious or if an exemption applies.

Further information

For more information on what 'excessive or malicious' means in practice, please refer to the section on key words and phrases below.

4.6. The right to be notified of processing

Article 6.1 of the PDPPL says:

> *''an individual shall have the right to… Be **notified of processing** the personal data thereof and the purposes for which such processing is to be conducted.''*

What does the right to be notified of processing mean in practice?

This article provides individuals with the right to be notified of processing about the collection and use of their personal data upon request. The right to be notified of processing means that an individual has the right to be told by a controller when the controller is using their personal data. This right is also known as the 'right to be informed'.

Article 6.1 requires the controller to inform the individual making the request of how their own personal data specifically is being processed.

This right is in line with the principle of transparency as set out in Article 3 of the PDPPL, which is the idea that personal data must be processed in a clear, open and honest way.

How can individuals exercise their right to be notified of processing?

Individuals should contact the controller and inform them that they wish to be notified of the personal data of theirs that the controller is processing.

Individuals can make a request for the correction of their personal data either verbally or in writing. The National Cyber Governance and Assurance Affairs recommends that, where a request is made verbally, individuals follow it up in writing to ensure that they have evidence of making the request for their records.

What information should the controller provide?

Individuals should be provided with general information by controllers of how their personal data will be processed at the time the controller collects their personal

data. This is often provided in the form of a privacy notice as per Article 9 of the PDPPL.

Controllers must provide the individuals making the request to be notified of processing with the following information regarding how the controller is processing their personal data:

- the categories of personal data concerned;
- the purposes for processing their personal data;
- the retention periods for their personal data or criteria for determining them;
- who it will be shared with; and
- where it will be processed.

When can a controller decide not to provide this information to an individual?
There are limited circumstances when controllers may not need to provide individuals with this information. This may be the case where:

- an individual already has the information; or
- it would involve a disproportionate effort to provide it to them.

Further information
For more information on Article 9 and privacy notices, please refer to the Guidelines on Privacy Notices for Regulated Entities.

4.7. The right to be notified of inaccurate disclosure

Article 6.2 of the PDPPL says:

> *''an individual shall have the right to… **Be notified** of any **disclosure of** any **inaccurate personal data** thereof.''*

What does the right to be notified of inaccurate processing mean in practice?
The right to be notified of inaccurate disclosure means that a controller must notify an individual in the event that an inaccurate record of their personal data has been shared with a third party.

What must controllers do in the event of inaccurate disclosure?
An individual should not have to take action to exercise their right to be notified of inaccurate disclosure; controllers should automatically inform an individual if they share inaccurate personal data about them with a third party upon discovering that such a disclosure has happened.

Organisations must provide the individual with:

- Details of the inaccuracy that has been shared;
- Provide the third party in question with an accurate record of the individual's personal data so that they can correct it.
- Proof that the inaccuracy has been corrected in the controllers systems.
- Proof that the third party in question has been furnished with an accurate record.

What should an individual do if a controller doesn't notify them in the event of inaccurate disclosure?

If an individual suspects that an organisation has shared an inaccurate record of their personal data with a third party but has not notified them or taken action to correct the record, the individual has the right to complain to both the organisation and to the National Cyber Governance and Assurance Affairs.

Further information

For more information on how to make a complaint to a controller or the National Cyber Governance and Assurance Affairs please refer to the Guidelines on Complaints for Individuals.

4.8. The right to access

Article 6.3 of the PDPPL says:

> *An individual may, at any time ''**Obtain a copy** of the personal data thereof after paying an amount that shall not exceed the service fee.''*

What does the right to access mean in practice?

The right to access means that individuals have the right to ask a controller:

- whether or not the controller is using or storing any of the individual's personal data; and
- for the controller to provide the individual with copies of their personal data.

Exercising this right is sometimes known as making a 'subject access request' or 'SAR'.

Why might an individual want to exercise their right to access?

An individual may wish to make a access request for access to find out:

- what personal data a controller holds about them;
- whether the information the controller holds is accurate and up to date;
- how the controller is using their personal data;
- who the controller is sharing their personal data with; and
- where they got the individual's personal data from.

This information may be required to enable individuals to exercise other rights under the PDPPL effectively. For example, if an individual learns personal data an organisation holds on them is incorrect, they may wish to exercise their right to request correction.

How can individuals make a request to access their personal data?

Individuals should contact the controller and inform the controller that they wish to be provided with access to their personal data that the controller is processing.

Individuals can make a request for the correction of their personal data either verbally or in writing. The National Cyber Governance and Assurance Affairs recommends that, where a request is made verbally, individuals follow it up in writing to ensure that they have evidence of making the request for their records.

What should individuals include in a request for access?

When making a request to exercise their right to access their personal data individuals should include:

- a clear description of what the request is concerning; for example by using 'subject access request' or 'right to access my personal data' as the email subject or letter heading;
- the date of making the request;
- the individual's full name (including any alternative names they are known by, if relevant);
- any other information used by the organisation to identify or distinguish the individual from other individuals, such as a customer account number or employee ID;
- their up-to-date contact details;
- an extensive list of what personal data that they want to access, based on what they need;
- any other relevant details such as dates or search criteria that will help the controller identify what the individual wants and locate their personal data; and
- how they would like to receive the information; for example via email or in hard copy to a postal address etc).

What should individuals not include in a request for access?

When making a request to exercise their right to access their personal data individuals should not include:

- other information, such as details about a wider customer service complaint. The request for access should be kept separate; or
- a request for all the information the organisation holds on them, unless that is what they need. This may lead to it taking the controller far longer to respond, or make it more difficult for the individual to locate the specific information they need when the controller does respond.

Can an individual ask a third party to make a request on their behalf?

Individuals can authorise someone else to make a subject access request on their behalf. Before doing so they should make sure that they are comfortable with the other person having access to some or all of their personal data.

Examples of third parties that commonly act on behalf of others are:

- someone with parental responsibility, or guardianship, where asking for information about a child or young person;
- a lawyer acting on their client's instructions; or
- a relative or friend who has been asked to help.

The controller must be satisfied that the third party has the permission of the individual concerned to make the request on their behalf. They may ask for formal evidence of this including written authorisation from the individual, or a more general power of attorney.

Are individuals required to pay a fee to make a request?

Controllers may charge a fee for providing copies of the data they hold on the individual, particularly if hard copies are requested. This amount must not exceed the service charge.

How should a controller respond to a request to exercise the right to access?
A controller must respond to a request within 30 calendar days.

If an individual has made a number of requests or their request is complex, they may need extra time to consider the request. Controllers can take up to an extra two months to respond to a complex case. If they are going to do this, they should let the individual know within one month that they need more time and why.

In their response, the organisation should confirm whether or not they are processing the individual's personal data and if they are they should provide them with copies of it.

The organisation should also include:

- what they are using the information for;
- who they are sharing the information with;
- how long they will store the information, and how they made this decision;
- details on the individual's rights to challenge the accuracy of their information, to have it deleted, or to object to its use;
- their right to complain to the National Cyber Governance and Assurance Affairs;
- details about where they got the individual's information from; and
- what security measures they took if they have transferred the individual's information outside of Qatar.

If there is something in particular an individual wishes to know, they should specify this in their request.

Can a controller refuse to provide an individual with access to their personal data?
Controllers will not always provide an individual with everything they asked for. They may only provide part of it, or they may not provide individuals with anything at all.

A controller may refuse to comply with an individual's request if the request is excessive or malicious or if an exemption applies.

Further information
For more information on what 'excessive or malicious' means in practice, please refer to the section on key words and phrases below.

5. Keywords and phrases

This section explains what each of the key words and phrases mean that are used to determine whether certain individual rights will apply.

5.1. What does "not necessary to achieve the purposes for which such personal data have been collected" mean?

When personal data is used for purposes that are not compatible with the original purpose they were collected for.

5.2. What does "beyond the extent required" mean?

When a controller holds more than the minimum amount of personal data about an individual than is required to fulfil their purpose; the controller should only hold the minimum amount of personal data required to fulfil their purpose, and no more.

5.3. What does "discriminatory" mean?

Data processing will be discriminatory if it leads to the unfair treatment of individuals leading to one group of people being treated differently, and often worse, than other groups.

5.4. What does "unfair" mean?

Data processing will be unfair if it is unduly detrimental, unexpected or misleading to the individuals concerned. To ensure fairness, the controller should only handle personal data in ways that people would reasonably expect and not use it in ways that have unjustified adverse effects on them.

5.5. What does "illegal" mean?

Not compliant with the PDPPL, or with any other law in the State of Qatar.

5.6. What does "no longer required" mean?

Where the purposes for processing have finished in line with the principle of purpose limitation.

5.7. What does "excessive or malicious" mean?

A request may be excessive if:

- it repeats the substance of previous requests; or
- it overlaps with other requests.

A request may be malicious if, for example:

- the individual making the request has no intention of exercising their right but is simply making the request in order to gain a benefit from the organisation in exchange for withdrawing the request.
- It is being used to harass an organisation with no real purpose other than to cause disruption to the organisation.

However, whether a request is excessive and/or malicious depends on the particular circumstances and should be assessed on a case by case basis. Organisations should consider each situation individually and assess whether the individual genuinely wants to exercise their rights in that case.

End of Document