State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

Individuals' Rights

PDPPL-02050205E

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-02050210E	Competent Authority Exemptions Guidelines for Regulated Entities (English)
PDPPL-02050211E	Controller Exemptions Guidelines for Regulated Entities (English)
PDPPL-02050208E	Data Privacy by Design and by Default Guidelines for Regulated Entities (English)
PDPPL-02050204E	Permitted Reasons Guidelines for Regulated Entities (English)
PDPPL-02050213E	Privacy Notice Guidelines for Regulated Entities (English)
PDPPL-02050212E	Records of Processing Activities (RoPA) Guidelines for Regulated Entities (English)
PDPPL-02050214E	Complaints 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 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) provides individuals with a number of rights in relation to their personal data.
- Controllers must put the appropriate policies and procedures in place to enable individuals to exercise these rights.
- Controllers must respond to individuals' requests to exercise their rights within 30 calendar days.
- Individuals can make a complaint to the National Cyber Governance and Assurance Affairs if they are not satisfied with how their rights are managed in accordance with the PDPPL.
- 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.
- If competent authorities are processing under Article 18 exemptions, they should see Guidelines on Exemptions Applicable to Competent Authorities for Regulated Entities.
- If controllers are processing under Article 19 exemptions, they should see Guidelines on Exemptions Applicable to Data Controllers for Regulated Entities.

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 has been developed to support controllers in understanding their obligations regarding these rights. They also set out the action's controllers should take to prepare to deal with requests from individuals.

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 action's 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."***

This provides individuals with the right to have their personal data protected and lawfully processed. Controllers have responsibility for protecting the personal data of individuals that they process, or that is processed on their behalf. Controllers are also responsible for processing personal data in compliance with the PDPPL.

What does this mean?

Protecting personal data means:

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

Lawful processing means:

- 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.

What do we need to do to comply?

Controllers must implement practices to ensure that personal data is protected and to ensure it is processed lawfully. These guidelines on individuals' rights set out what controllers must do to provide individuals with control over their personal data.

For information on keeping personal data secure and what controllers need to do, please see the Data Privacy by Design and by Default Guidelines which include information on appropriate measures for the protection of personal data.

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 this mean?

This means that where controllers are relying on an individual's explicit written consent to process their personal data as per Article 4 PDPPL, the individual has the right to withdraw this consent.

What do we need to do to comply?

Controllers must:

- enable individuals to withdraw their previously given consent at any time;
- inform individuals that they can withdraw their consent at any time;
- inform individuals how they can withdraw their consent;
- cease processing the personal data once an individual has withdrawn their consent;
- not make it difficult for an individual to request the withdrawal of their consent;
- act on requests for withdrawal of consent as soon as possible; and
- not penalise individuals for withdrawing their consent. For example, an individual must not suffer any detriment as a result of having withdrawn their consent.

For further information on explicit written consent please see the Permitted Reasons Guidelines 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 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.

When does this right apply?

The right to object applies in the following circumstances:

- when the processing of the 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 personal data:
    - beyond the extent required;
    - in a way that is discriminatory;
    - unfair; and/or
    - illegal.

For more guidance on what these terms mean in practice please see refer to the key words and phrases below.

What do we need to do to comply?

When complying with the right to object, controllers should consider the following:

- when an individual exercise their right to object, the controller should confirm that one or more of the above circumstances exist. If this is confirmed, the controller should erase their personal data unless this is not appropriate in the circumstances.
    - Erasure of the personal data will not always be the most appropriate response to a valid objection; for example, it may not be appropriate if the controller needs to retain the data for a contractual or legal obligation, or to demonstrate that explicit consent was obtained.
- The right to object is only applicable in certain circumstances as set out above.
    - Individuals must give a specific reason why they object to the processing of their personal data; and
    - controllers must cease processing an individual's personal data unless they can demonstrate that their reason does not fall under one of these circumstances or if the request is excessive or malicious.
- Individuals may object to decisions that are made based solely on automated processing where such processing may be discriminatory;
    - an appropriate response to such a request is to ensure there is human intervention to the automated process; and
    - a competent person should analyse the decisions made, in particular to make sure they are not discriminatory, and must change the decision if it is appropriate to do so.

For more guidance on what 'excessive or malicious' means in this context, please see key words and phrases on page 19 below.

4.4. The right to erasure

Article 5.3 of the PDPPL says:

> *''Request **omission or erasure** of the Personal Data thereof in any of the cases referred to in the preceding two items , upon cessation of the purpose for which the processing has been conducted, or where all justifications for maintaining such Personal Data by the Controller cease to exist.''*

This provides individuals with the right to have their personal data erased (in whole or in part). This right is also known as the 'right to be forgotten'.

When does this right apply?

The right to erasure will apply in the following circumstances:

- *When an individual withdraws their consent*

Where the controller is relying on an individual's 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.

Exemptions

Even in the above circumstances, the right to erasure will not apply if an exemption is applicable or if the request is deemed excessive or malicious.

If this is the case, the controller can either fully or partly refuse to comply with the individuals request.

For further information on what 'excessive or malicious' means in this context, please see key words and phrases on page 19 below.

For further information on exemptions please see Guidelines on Exemptions Applicable to Data Controllers (under Article 19) for Regulated Entities.

What do we need to do to comply?

- Individuals can make a request in writing or verbally. Controllers should document requests made, including those made verbally.
- A request can relate to either all the personal data controllers hold on an individual, or just to some of the data controllers hold on them.
- Controllers must respond to requests for erasure within **30 calendar days** from receiving them.

Where controllers accept the erasure request:

- Once a request is received and the controller confirms that the right applies, the controller must take all reasonable steps to delete the personal data.
- Controllers should inform any third parties they have shared the data with about the request for erasure, unless this involves a disproportionate effort or is impossible.
- If the data has been made public online – such as on social networks, forums or websites – then controllers must take reasonable steps to inform the people with responsibility for these sites to erase links or copies of that data.

Where controllers reject an erasure request:

- If, having considered the request, controllers decide they are not obliged to erase the data (because one of the above circumstances does not exist, because the request is excessive or malicious or because an exemption applies), controllers should still respond to the individual.
- Controllers should explain why they believe they are not required to erase the data and should inform the individual about their right to complain about their decision, both to the controller and / or the National Cyber Governance and Assurance Affairs.

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.''*

This provides individuals with the right to request that controllers correct the personal data they hold about them. This includes requests to both:

- rectify inaccurate personal data (e.g. personal data that is incorrect or misleading as to a matter of fact); and/or
- complete personal data if it is incomplete.

This right is in line with the principle of accuracy as set out in Article 10 of the PDPPL, which requires controllers to ensure that the personal data held on individuals is accurate and kept up to date.

What do we need to do to comply?

Individuals can make a request verbally or in writing and controllers should respond to requests for correction within **30 calendar days** from receiving them.

The PDPPL states in Article 5.4 that individuals must be able to provide proof of the accuracy of the personal data they provide to controllers as a part of any request. Controllers should therefore take reasonable steps to satisfy themselves of the proof provided to them and should develop a process to do so that they routinely follow.

What steps are reasonable will depend upon the nature of the personal data in question and what it will be used for. The more important it is that the personal data is correct, the greater the effort should be to check its accuracy.

If, after taking such reasonable steps, the controller is satisfied that the personal data is accurate as it is and that the proof provided by the individual is insufficient to prove otherwise, the controller must inform the individual that they will not be amending the data and should explain why this is. The controller should also inform the individual of their right to make a complaint to the National Cyber Governance and Assurance Affairs as per Article 26 PDPPL.

When else may we reject a request?

Controllers may also reject a request where the request is deemed excessive or malicious, or if an exemption applies.

For further information on what 'excessive or malicious' means in this context, please see key words and phrases on page 19 below.

For more information on exemptions please see Guidelines on Exemptions Applicable to Data Controllers (under Article 19) for Regulated Entities.

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 of the Personal Data thereof and the purposes for which such processing is conducted"*

This article provides individuals with the right to be informed about the collection and use of their personal data upon request.

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. It also ties in with Article 9 of the PDPPL concerning privacy notices.

What do we need to do to comply?

Controllers may already be providing individuals with general information of how they process personal data at the time they collect their personal data. This is often provided in the form of a privacy notice as per Article 9 of the PDPPL.

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

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.

For more information on privacy notices please see Privacy Notice Guidelines 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.''*

This provides individuals with the right to be notified when a third party has been given inaccurate information concerning the individual's personal data.

What do we need to do to comply?

To comply with this right, controllers should:

- provide the concerned individual with details of the inaccuracy disclosed;
- provide the third party in question with an accurate record of the personal data so that they can correct it; and
- once rectified, the controller should provide the individual with proof that the inaccuracy has been corrected.

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 charge.''*

This gives individuals the right to obtain a copy of the personal data controllers hold on them. Such requests are also known as subject access requests.

Exercising such a right helps individuals to understand how and why controllers are using their data, and to check that controllers are doing so lawfully.

Individuals may make a subject access request verbally or in writing. Controllers must respond to requests for access within **30 calendar days.**

Controllers may charge individuals a fee for providing them with copies of the data they hold on them, but such amount must not exceed the service charge.

Such a fee must be proportionate to the cost of complying with the request, not elicit a profit and must not make such a request prohibitively expensive to individuals.

What do we need to do to comply?

To comply with the right to access controllers should:

- Know how to recognise a request for access and understand when the right to access applies.

- Understand that requests can be made to any part of their organisation, including via social media, and that requests do not need to be made to a specific department or person.
- Consider inviting individuals to use a standard subject access request form to make requests, (but keep in mind that requests submitted by other means will still be valid).
- Have policies and procedures in place for how to respond to requests they receive, covering both when requests are received verbally and in writing.
- Provide the information in a concise, transparent, intelligible and easily accessible form, using clear and plain language. This is particularly important where a request is received from a child or their guardian.
- Understand that an individual is only entitled to their own personal data, and not to information relating to other people (unless the information is also about them or they are acting on behalf of someone e.g. a guardian of a child).
- Understand that upon receiving a request, it is not acceptable to amend or delete the data if they would not otherwise have done so.

If the controller has doubts about the identity of the individual making a request, the controller may ask them for more information. Controllers must not ask them for any more information than that which is necessary to confirm who they are.

If the controller processes a vast amount of information on an individual, the controller may ask them to clarify the information or processing activities that their request relates to before responding to the request. However, the controller cannot ask them to narrow their request, and they must still respond within the timeframe of 30 calendar days.

Requests made on behalf of others

Individuals may wish to make a subject access request via a third party. This could be an individual's lawyer acting on their behalf, or simply an individual asking a friend or family member to act for them.

In these cases, the controller must be satisfied that the third party is entitled to act on behalf of the individual, but the burden is on the third party to prove that this is the case. This proof is likely to be in the form of a written authority.

When else may we reject a request?

Controllers may also reject a request where the request is deemed excessive or malicious, or if an exemption applies.

For more information on exemptions please see Guidelines on Exemptions Applicable to Data Controllers (under Article 19) for Regulated Entities.

5. Key words and phrases

The rights to object and to erasure are qualified rights and only exist under certain circumstances. This section explains what each of the key words and phrases mean that are used to determine whether each of these rights apply.

What does "no longer necessary to achieve the purposes for which such personal data have been collected" mean?

When the processing of the individual's personal data is no longer necessary to achieve the purpose for which the controller collected it or when the purpose for which the personal data was collected has ceased to exist.

What does "beyond the extent required" mean?

When the 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.

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.

Individuals should provide the controller with evidence of how they have been treated differently and unfairly as a result of the data processing in question.

What does "unfair" mean?

Data processing will be unfair if it is unduly detrimental, unexpected or misleading to the individuals concerned. To ensure fairness, controllers 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.

What does "illegal" mean?

Data processing will be illegal if it is not compliant with the PDPPL, or with any other law in the State of Qatar.

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 controller in exchange for withdrawing the request; and/or
- It is being used to harass a controller with no real purpose other than to cause disruption to the controller.

However, whether a request is excessive and/or malicious depends on the particular circumstances and should be assessed on a case by case basis.

Controllers should consider each situation individually and assess whether the individual genuinely wants to exercise their rights in that case.

6. General guidelines on dealing with requests

This section sets out the steps that controllers should take to deal with requests made by individuals wishing to exercise their rights. Controllers should make sure they are aware of which rights apply in all circumstances and which are conditional, and make sure that this is understood across their organisation.

They should respond to requests within 30 calendar days of receipt either to confirm that they have complied with the request or to inform the individual that they do not believe action needs to be taken and their justification for this judgement.

6.1. Identifying personal data

- Controllers should be able to identify all personal data that relates to an individual in the event of receiving a request.
- This means that controllers need to know where personal data is located across their entire IT estate.
- This requires controllers to have a record of the personal data they process. Controllers should develop a data processing register as set out in the Records of Processing Activities guidelines.

6.2. Policies, procedures and systems

- Controllers should establish a procedure that they follow for when requests are received from individuals, as well as for recording these requests. This should include a process to be followed when requests are made verbally.
- Controllers should establish a procedure to verify the ID of the individual making the request, to check that they are who they say they are.
- Internal policies and procedures regarding responding to individual rights requests should set out:
    - that the controller will comply with the PDPPL by enabling individuals to exercise their rights;
    - the controller's process for receiving, carrying out and recording individual rights requests as soon as possible after receipt, and within 30 calendar days;
    - the role of employees in complying with these requests;
    - how the controller will interact with other controllers and processors to enable individuals to exercise their rights fully;
    - the controller's approach to any exemptions that may mean they do not have to comply with certain requests; and
    - the controller's approach to documenting their activities regarding individual rights requests so that they can demonstrate their compliance with the PDPPL, in line with the principle of accountability.

- Controllers should implement formal training to ensure all staff are aware of how to identify an individual rights request and how to follow the procedure for responding to requests.
- Controllers should confirm that their systems enable them to take the action required to comply with requests.
- Controllers should have a process in place for individuals to make complaints to them, as well as an internal procedure for how such complaints are dealt with. For more information, see Complaints Guidelines for Regulated Entities.

6.3. Other considerations

- Once a request has been dealt with, the controller should inform the individual of the action they have taken and, if applicable, that they consider the request closed. Where the controller has taken no action, they must inform the individual and include the reason as to why this is; e.g. the exception that applies, and/or why the right is not applicable in the circumstances.
- Controllers should maintain a record of how all requests are dealt with so that they can demonstrate compliance with PDPPL requirements. At a minimum they should record:
    - the date of receipt and closure of the request;
    - any decisions made on how to respond as well as the reasons for such decisions; and
    - evidence that the controller has complied with their requests.
- When responding to requests controllers should take care to:
    - not provide personal data that could negatively impact another individual's rights;
    - not provide personal data that could cause serious harm to the physical or mental health of the individual or to any other person; and
    - not provide personal data that could prejudice an investigation or tip off a suspect in an investigation; for example, personal data linked to suspected money laundering, or suspicious transactions.
- If individuals are not satisfied with how the controller has handled their request, they can make a complaint to the National Cyber Governance and Assurance Affairs as the data privacy regulator.

End of Document