State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

Personal Data Breach Notifications

PDPPL-02050217E

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-02050208E	Data Privacy by Design and by Default Guidelines (English)
PDPPL-02050206E	Data Privacy Impact Assessment (DPIA) Guidelines for Regulated Entities (English)
PDPPL-02040402E	Personal Data Breach Notifications Form 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 "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

- A data breach is the loss, alteration, destruction or disclosure of data. Breaches can occur due to deliberate or accidental reasons. Where personal data is involved, it is a personal data breach.
- Personal data breaches can cause serious damage to individuals, whether physical, emotional or material being used, for example, to enable theft or discrimination or to cause a nuisance to individuals.
- Controllers must put appropriate precautions in place to prevent personal data breaches. Controllers should be able to detect breaches, be able to conduct triage activities in a reasonable timeframe and be able to assess whether the breach may cause serious damage to individuals.
- Controllers should conduct personal data breach response exercises regularly. This should be a part of their information security framework.
- Controllers must notify the National cyber governance and assurance affairs and individuals of a personal data breach within 72 hours of becoming aware of the breach where the breach can cause serious damage to individuals.
- Failure to report a personal data breach to the National cyber governance and assurance affairs or individuals as required could result in a penalty of up to QAR 1,000,000 per violation under Article 23 of the PDPPL.
- Failure to put in place appropriate precautions commensurate to the nature and importance of the personal data could result in a penalty of up to QAR 5,000,000 per violation under Article 24 of the PDPPL.
- Failure of a processor to inform a controller of a personal data breach where a risk arises in any way could result in a penalty of up to QAR 5,000,000 per violation under Article 24 of the PDPPL
- If a controller is within the scope of other international personal data laws or regulations (such as the European Union's General Data Protection Regulation) the controller should consider breach reporting requirements under these laws as well as under the PDPPL.

2. Introduction

The PDPPL requires controllers to notify individuals and the National cyber governance and assurance affairs of any breach that "may cause serious damage" to an individual's privacy or personal data. This could be a breach of security, for example the theft of personal data, or a breach of the precautions to protect personal data and privacy, for example where administrative precautions such as policies and procedures are not followed by employees or technical precautions such as encryption have been found not to be effective.

These guidelines have been prepared by the Compliance and Data Protection (National cyber governance and assurance affairs) Department to provide controllers with information on precautionary measures they can take to reduce the likelihood of a personal data breach, their obligations to respond to a breach in the event that one occurs and the requirements to report such a breach to the National cyber governance and assurance affairs depending on its nature.

The requirements for the prevention, management and reporting of breaches can be found in Articles 11(5), 13 and 14, and are explained in more detail below.

3. What is a personal data breach?

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

Some examples of personal data breaches are as follows:

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

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

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

The above examples are not exhaustive but are indicative of the types of breaches and consequences that controllers must put precautions in place to prevent and mitigate.

4. What does the PDPPL say about personal data breaches?

Article 11.5 of the PDPPL states:

> *"Develop and implement an internal effective Personal Data management system, and **report any breach of protection measures** thereof."*

Article 13 of the PDPPL states:

> *"The Controller and the Processor shall adopt all **necessary precautions to protect Personal Data** against loss, damage, change, disclosure and/ or illegal / inadvertent access thereto and/ or use thereof.*
>
> *Precautions so adopted shall be commensurate to the nature and the importance of the Personal Data under protection. **The Processor shall forthwith notify the Controller of any breach of such precautions** or where **any risk of threats arises to Personal Data in any way**."*

Article 14 of the PDPPL states:

> *"The Controller **shall inform both the relevant individual and Competent Department** upon **occurrence of a breach of such precautions**, **if this breach may cause serious damage** either to Personal Data or relevant individual privacy."*

In summary, the PDPPL says the following about personal data breaches:

- Controllers should take appropriate precautions to prevent and reduce the likelihood and impact of breaches.
- Controllers should be able to detect a breach if it occurs and immediately assess the potential for serious damage to individuals.
- Controllers should report the personal data breach to the National cyber governance and assurance affairs without delay and within 72 hours of becoming aware of it, if the personal data breach could cause damage to individuals' personal data or privacy.
- Controllers should notify the individuals of the personal data breach without delay and within 72 hours of becoming aware of it if the personal data breach could cause serious damage to their personal data or privacy.

5. What precautions can controllers take to reduce the likelihood of a personal data breach?

There are numerous precautions that controllers can take to reduce the likelihood of a personal data breach, with new precautions being developed regularly. Controllers are required to take administrative, technical and financial precautions to protect personal data and individuals' privacy. Comprehensive guidance on such precautions can be found within the Data Privacy by Design and by Default Guidelines for Regulated Entities.

Examples of precautions controllers can implement, specifically with regard to preventing personal data breaches, are listed below.

Implement a robust information security framework

Controllers should implement a robust information security framework, where data (including personal data) is classified and kept secure using security measures that are commensurate to the risk of damage that a breach could cause to individuals' privacy or personal data.

Setup a personal data breach response framework

Controllers should prepare for potential breaches by implementing a personal data breach response framework. This framework should allocate roles and responsibilities that employees must fulfil in the event of a breach (see next item) and provide the necessary tools and guidance for them to respond effectively to the personal data breach. A controller's ability to respond to a breach efficiently and effectively increases in line with the level of preparations made. A personal data breach response framework should include appropriate guidance for:

1. becoming aware of a personal data breach;
2. notifying the relevant individual(s) in the organisation;
3. communicating to employees about the personal data breach with instructions on confidentiality;
4. conducting triage activities;
5. setting up a breach response team;
6. determining the extent to which personal data is breached;
7. conducting an assessment of serious damage to individuals;
8. assessing notification requirements and notifying the National cyber governance and assurance affairs and individuals;
9. closing the personal data breach; and
10. documenting the breach and lessons learnt to reduce a repeat occurrence.

Define roles and responsibilities for personal data breach response

Controllers should define who is responsible for conducting triage activities after a breach is detected, assessing potential damage to the individual/s, communicating to the National cyber governance and assurance affairs and affected individuals, performing activities to manage and close the breach.

Conduct a Data Privacy Impact Assessment (DPIA) for relevant processing activities

Controllers should carry out DPIAs before carrying out new processing activities. They are particularly important where the processing may cause serious damage to the individuals to whom the personal data relates. One of the risks to be identified when carrying out the DPIA is the risk of a breach. Measures to prevent or respond to the personal data breach, including any specific measures that need to be taken for that particular processing activity, should be identified too.

Train employees on personal data breach detection and notification

Controllers should arrange for regular training and awareness sessions on privacy which should cover personal data breaches and the appropriate procedures to be followed upon the detection of a breach. Employees should know how to identify a personal data breach and, if they do so, who to inform within the controller's organisation.

Training in privacy and personal data breaches is an essential administrative precaution for protecting personal data. If employees are not aware of how to recognise a personal data breach such breaches may go undetected.

Define responsibilities of the controller and the processor in the event of a breach in contracts

Where a controller has engaged a processor to process personal data on their behalf, the controller should ensure that, in their contracts and data processing agreements, they have clearly defined the obligations of each party in the event of a personal data breach.

For example, if the processor suffers a personal data breach, the controller should be informed immediately if the data that has been breached consists of personal data that the controller has entrusted to the processor for processing in line with Article 13 of the PDPPL.

Conduct breach response exercises and drills regularly to test breach response plans

Breach response plans are extremely important to be able to effectively respond to personal data breaches when they occur. Controllers should consider conducting simulated 'tabletop' breach response exercises to practice, test and improve breach response plans periodically.

6. When should controllers notify the National cyber governance and assurance affairs and individuals of a personal data breach?

Article 14 of the PDPPL requires controllers to notify the National cyber governance and assurance affairs and individuals of a breach if the breach may cause damage to individuals' privacy or personal data.

The controller should notify the National cyber governance and assurance affairs and individuals of a personal data breach within 72 hours of becoming aware of it.

The controller is responsible for assessing whether a breach may cause serious damage to individuals' privacy or personal data. When controllers become aware of a personal data breach, they should work to contain the breach in parallel with assessing its potential impact on individuals.

What if the controller is aware of a breach but does not have all the relevant information?

It will not always be possible to investigate a personal data breach fully within 72 hours to understand the nature and circumstances of the breach or identify the required actions to protect individuals against serious damage to their privacy or personal data.

Controllers should notify the National cyber governance and assurance affairs with the information they have available within 72 hours if they think it is likely to cause damage to individuals. They should include the reasons why they are not able to provide all the required information within 72 hours and set out how and when they will be able to provide further information.

Controllers should make all reasonable efforts to expedite the investigation into the breach such as ensuring the required resources are made available to the investigating team.

How do controllers assess whether a personal data breach could cause serious damage to individuals?

In assessing the damage caused by a personal data breach, controllers must pay particular attention to the negative consequences for individuals affected by the breach. A breach may cause individuals to be impacted negatively in a number of ways including adverse effects such as emotional distress, and physical or material damage. Examples of processing that, when impacted by a breach, could increase the severity of damage to individuals are:

- processing any special nature personal data;
- using a new innovative technology or an existing technology in a new way;
- carrying out automated decision-making which leads to a decision to limit an individual's access to a product, service, opportunity or benefit i.e. decisions made by a computer without human involvement;
- collecting personal data via third parties instead of directly from individuals;

- tracking individuals or monitoring their behaviour (e.g. CCTV, online browsing patterns, GPS location tracking);
- undertaking a cross-border personal data transfer i.e. transferring personal data outside of the State of Qatar;
- using personal data to target direct marketing at individuals;
- marketing or provision of goods or services to children (e.g. sending promotional emails to children) without parental consent; and
- carrying out a processing activity that is new to the controller's industry.

It is essential that controllers have procedures in place to conduct an assessment of damage caused by a breach to individuals in a timely yet robust manner. If controllers have complied with Articles 11(1) and 13 of the PDPPL by conducting DPIAs on their processing activities, and documented these in their Record of Processing Activities (RoPA), they will already have assessments of potential damage that a breach could cause at a processing activity level. These serve as a valuable input into any breach assessment.

For more information on what may cause serious damage to individuals, please refer to the Guidelines on Data Protection Impact Assessments (DPIAs) for Regulated Entities.

Controllers are accountable for their decision making and should document the rationale of their decision on whether or not to report a breach to the National cyber governance and assurance affairs and individuals. This is particularly important if the controller decides not to report a breach.

If the controller incorrectly concludes that the breach could not cause serious damage when it could and subsequently decides not to notify the National cyber governance and assurance affairs or individuals when they should, the controller may be found to be in non-compliance with the PDPPL.

If the controller is found to be in non-compliance with the Article 14 breach reporting requirements, they may be liable for a penalty under Article 23 of the PDPPL.

7. How should controllers notify the NATIONAL CYBER GOVERNANCE AND ASSURANCE AFFAIRS ?

Controllers should notify the National cyber governance and assurance affairs via the breach notification page on the National cyber governance and assurance affairs website using the Breach Notification Form.

The breach notification must:

- detail the nature of the personal data breach, including, to the extent possible, the categories of individuals concerned, the types of personal data involved and an estimated number of individuals and personal data records concerned;
- include the name and contact details of the company's primary responsible person for privacy related matters or information on who the National cyber governance and assurance affairs can contact to obtain further information;
- describe the consequences likely to occur due to the personal data breach; and
- describe the action(s) that the controller has taken or proposes to take to address the personal data breach, including, where appropriate, actions to mitigate the possible adverse effects of the personal data breach.

If controllers do not report the personal data breach to the National cyber governance and assurance affairs and the National cyber governance and assurance affairs later becomes aware of the breach through another source, this will likely result in an investigation by the National cyber governance and assurance affairs .

8. How should controllers notify individuals?

The communication to the individual should be made directly to them and describe nature of the personal data breach in clear and plain language the and should include the following information at a minimum:

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

Notification of affected individuals is particularly important when the breach could cause serious damage to the affected individuals' privacy or personal data.

Controllers are accountable for their decision making and should document the rationale of their decision on whether or not to notify affected individuals of a breach involving their personal data. This is particularly important if the controller decides not to report a breach.

Controllers may wish to engage with the National cyber governance and assurance affairs prior to notifying individuals of a personal data breach to consult on the manner and content of communications.

9. What will the National cyber governance and assurance affairs do after a controller notifies it of a personal data breach?

Once the controller notifies the National cyber governance and assurance affairs, the National cyber governance and assurance affairs may do any or all of the following:

Establish the circumstances of the breach

This may include establishing:

- how the breach occurred;
- when the breach began;
- when the controller became aware of the breach;
- when the controller contained the breach; and/or
- which parts of the business were affected.

Establish the nature of the compromised data

Details of the compromised data may include the:

- categories or nature of the compromised personal data;
- extent of the compromised personal data;
- location of the compromised personal data;
- categories and number of individuals affected; and/or
- details of any adverse impact on individuals.

Identify and assess the precautions the controller has in place to prevent breaches

Examples of evidence of precautions the National cyber governance and assurance affairs would expect to see in place are not limited to but include:

- a data privacy and protection policy;
- an information security policy;
- details of technical breach prevention precautions e.g. encryption, firewalls etc; and
- evidence of periodic mandatory staff training in data privacy protection and breach prevention.

Investigate the involvement of third parties if applicable

This may include assessing:

- the contractual agreement in place between the controller and relevant third parties;
- the extent controller verified the appropriate precautions of the processors and their compliance to the controller's instructions;

- whether the controller understand how the data would be held and processed; and/or
- the controller's approach to due diligence regarding processors and any sub-processors?

Review the controller's remediation and notification efforts

This may include assessing:

- the steps taken by the controller to contain the breach and mitigate any risk of damage to privacy or personal data of individuals;
- the timeliness and robustness of any assessments of the damage caused to individuals by the breach;
- the timeliness and nature of the notification to the National cyber governance and assurance affairs;
- the timeliness and nature of any notifications to individuals; and/or
- details of any complaints made by affected individuals.

10. What should controllers do after they have notified the NATIONAL CYBER GOVERNANCE AND ASSURANCE AFFAIRS and / or individuals of the personal data breach?

Controllers should continue to work towards containing and resolving the personal data breach in accordance with their internal procedures. In parallel they should ensure that they document the breach effectively and prepare for any increased activity required to handle requests and complaints from individuals.

Document details of the breach and lessons learnt

Full details of the personal data breach and any lessons learnt should be fully documented with the aim of reducing the likelihood of a similar breach occurring again in the future. This involves collecting all the facts of the breach, assessing any control weakness that could cause the breach to continue or occur again, determining any remediation required and documenting details of the personal data breach from the point of identification till closure. Controllers should also continue to provide information to the National cyber governance and assurance affairs and individuals as necessary.

Prepare for an increase in individuals rights requests and complaints

Controllers should be prepared to receive a higher volume of data protection requests or complaints as a result of a breach, particularly in relation to access requests and erasure. They should have a contingency plan in place to deal with them. It is important that these continue to be dealt with alongside any work that has been generated specifically in order to deal with the personal data breach. Controllers should also consider how you might manage the impact on individuals, including explaining how they may pursue compensation or avail of any mitigating products or services that will be provided should the situation warrant it.

11. What else should controllers consider in relation to personal data breaches?

Be aware of reporting requirements in other jurisdictions

If a controller is within the scope of other international personal data laws or regulations (such as the European Union's General Data Protection Regulation) the controller should consider breach reporting requirements under these laws as well as under the PDPPL.

Controllers may wish to engage with the National cyber governance and assurance affairs prior to notifying international privacy regulators of a personal data breach to consult on the manner and content of communications.

Be aware of potential fines that the controller and their processors could be subject to

The PDPPL sets out fines that controllers and processors may be liable to pay if they do not comply with requirements regarding personal data breaches. The potential fines are set out below:

- Failure to report a personal data breach to the National cyber governance and assurance affairs or individuals as required could result in a penalty of up to QAR 1,000,000 per violation under Article 23 of the PDPPL.
- Failure to put in place appropriate precautions commensurate to the nature and importance of the personal data could result in a penalty of up to QAR 5,000,000 per violation under Article 24 of the PDPPL.
- Failure of a processor to inform a controller of a personal data breach where a risk arises in any way could result in a penalty of up to QAR 5,000,000 per violation under Article 24 of the PDPPL.

End of Document