State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

# Exemptions Applicable to Data Controllers (under Article 19)

## PDPPL-02050211E

## 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-02050204E** | Permitted Reasons Guidelines for Regulated Entities (English) v1.0 |

## 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 "Exemptions Applicable to Data Controllers 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 6
2. Introduction 7
3. Who do the exemptions under Article 19 apply to? 8
4. When do the Article 19 exemptions apply? 9
   4.1. What does the PDPPL say about exemptions? 9
5. In what cases do the Article 19 exemptions apply? 10
   5.1. Executing a task related to the public interest as per the law 10
   5.2. Implementing a law or an order rendered by a competent court 10
   5.3. Protecting vital interests of individuals 10
   5.4. Achieve purposes of scientific research for public interest 11
   5.5. Gathering necessary information for investigation into a crime in response to an official request by investigative bodies 12
6. What obligations does each exemption relieve controllers of? 13
   6.1. Exemption from Article 4 - Permitted reason for processing 13
   6.2. Exemptions from Article 5 (1), (2), (3) and Article 6 - Obligation to comply with some individual rights 13
7. How do exemptions work in practice? 14

## 1. Key points

- The purpose of these guidelines is to explain the exemptions from certain obligations that apply to controllers in certain circumstances under the Personal Data Privacy Protection Law (PDPPL), the impact of such exemptions and how controllers should identify situations in which these exemptions apply to them.
- The PDPPL exempts controllers from needing to identify a permitted reason for processing under Article 4 and from obligations regarding some of the rights under Article 5 (1), (2) and (3), and Article 6 in certain circumstances.
- Whether or not the Controller can rely on an Article 19 exemption for certain processing activities depends on why the Controller processes the personal data.
- Controllers should not routinely rely on the exemptions; they should consider them on a case-by-case basis.
- If no exemption covers what a controller does with personal data, they need to comply with the PDPPL as normal.
- Controllers should keep a record of the processing activities for which they are applying an exemption and their basis for doing so.

## 2. Introduction

The PDPPL exempts controllers that are processing personal data from complying with Article 4, Article 5 (1), (2) and (3), and Article 6 when processing of personal data in the following cases:

- Executing a task related to the public interest as per the law.
- Implementing a legal obligation or an order rendered by a competent court.
- Protecting vital interests of individuals.
- Achieving purposes of scientific research for public interest.
- Gathering necessary information for investigation into a criminal offence in response to an official request by investigative bodies.

The exemptions for controllers can be found under Article 19 of the PDPPL and each exemption is explained in more detail below.

## 3. Who do the exemptions under Article 19 apply to?

The exemptions under Article 19 apply to all Controllers in the State of Qatar.

A Controller is a natural and/ or legal person who, whether acting individually or jointly, determines how Personal Data may be processed and determines the purpose(s) of any such processing.

An organisation is a Controller with respect to a processing activity if they are the main decision-maker exercising overall control over why and how personal data is processed.

## 4. When do the Article 19 exemptions apply?

Article 19 relieves controllers of some of the obligations set out in the PDPPL when processing for specific purposes. These obligations are the requirement to have a permitted reason for processing personal data under Article 4, and the requirement to comply with some of the individual rights, specifically those set out under Articles 5 (1), (2), (3) and 6.

### 4.1. What does the PDPPL say about exemptions?

Article 19 of the PDPPL says:

> *"The Controller shall be exempted from the provisions of Articles (4), (5\ Items 1, 2, and 3) and (6) hereof, in any of the following cases:*
>
> 1. *Executing a task related to the public interest as per the law.*
> 2. *Implementing a legal obligation or an order rendered by a competent court.*
> 3. *Protecting vital interests of Individuals.*
> 4. *Achieving purposes of scientific research which is underway for public interest.*
> 5. *Gathering necessary information for investigation into a criminal offense, upon an official request of investigative bodies."*

Even where controllers are processing personal data for one of these purposes and have exemptions under Article 19, they must still comply with all other obligations in respect of the PDPPL.

Guidance on each case in which controllers are exempted is set out below.

## 5. In what cases do the Article 19 exemptions apply?

### 5.1. Executing a task related to the public interest as per the law

The exemptions under Article 19 apply in this case if a controller processes personal data for the purpose of executing a task related to the public interest. A controller is doing this if they are either:

- carrying out a specific task in the public interest which is laid down by law; or
- exercising official authority (for example, a public body's tasks, functions, duties or powers) which is laid down by law.

The relevant task or authority must be laid down by law. This will most often be a statutory function, although it does not need to be an explicit legal provision and will also include functions or powers set out in statute or statutory guidance.

A controller does not need specific legal authority for the particular processing activity. The point is that their overall purpose must be to perform a public interest task or exercise official authority, and that overall task or authority has a sufficiently clear basis in law.

### 5.2. Implementing a law or an order rendered by a competent court

The exemptions under Article 19 apply in this case if a controller is required by law, or court order, to process personal data in relation to such an order.

### 5.3. Protecting vital interests of individuals

The exemptions under Article 19 apply in this case where it is necessary for controllers to process personal data in order to protect an individual's vital interests.

Vital interests are intended to cover only interests that are essential for someone's life. This exemption is very limited in its scope, and generally only applies to matters of life and death.

It is likely to be particularly relevant for emergency medical care, when a controller needs to process personal data for medical purposes, but the individual is incapable of giving consent to the processing. It is less likely to be appropriate for medical care that is planned in advance.

Vital interest is also unlikely to be the appropriate basis for processing personal data on a larger scale. However, vital interests might apply where a controller is processing on humanitarian grounds such as monitoring epidemics, or where there is a natural or man-made disaster causing a humanitarian emergency.

In most cases the protection of vital interests is likely to arise in the context of health data. This is one of the categories of special nature personal data, which means controllers will also need to identify a condition for processing personal data of a special nature.

One of the conditions for processing special nature category data is where it is necessary to protect someone's vital interests. However, this only applies if the individual is physically or legally incapable of giving consent. Explicit consent will be more appropriate in many cases, and controllers cannot in practice rely on vital interests for special nature data (including health data) if the data subject refuses consent, unless they are not physically or mentally competent to do so.

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

### 5.4. Achieve purposes of scientific research for public interest

This case for exemption only applies when the scientific research is in the public interest.

For the purposes of the PDPPL, the processing of personal data for scientific research purposes should be interpreted in a broad manner to include for example, technological development and demonstration, fundamental research, applied research and privately funded research.

It is important that any public interest test considers how best to balance public interest with the PDPPL data privacy principles and rights of individuals in conducting market and social research. Public interest can cover research which is of a wide benefit to society and the economy, and that it covers research carried out by both government, and commercial and non-commercial researchers, such as those based in university research centres, think-tanks, charities, not-for-profit and commercial research organisations.

Controllers within these organisations should carry out a balancing test, assessing the public interest in light of the potential impact on individual rights and freedoms. The approach to this will be similar to that used in assessing a legitimate interest. Issues to consider include:

- What is the public interest being pursued?
- Is the processing necessary for this public interest?
- Does the impact on individual's rights and freedoms override the public interest being pursued?

A balancing test should be carried out in conjunction with a Data Privacy Impact Assessment (DPIA) and based on information in the Record of Processing Activities (RoPA) to ensure that all documentation is aligned and the processing activity is considered in its totality.

The National Cyber Governance and Assurance Affairs has created a template to enable controllers to carry out a balancing test called the Legitimate or Public Interest Balancing Test which is available on the website data privacy guidance hub.

#### Appropriate safeguards for the protection of privacy

When relying on the scientific research for public interest exemption, controllers must have appropriate safeguards in place. These include but are not limited to:

- measures to protect the rights and freedoms of individuals;
- adequate technical and security measures which entrench the principle of data minimisation and the use of pseudonymised and anonymised data as default; and
- compliance with recognised ethical safeguards and frameworks.

Controllers relying on this exemption must still ensure that they are processing the personal data in line with the principle of transparency as set out in Article 3 of the PDPPL.

### 5.5. Gathering necessary information for investigation into a crime in response to an official request by investigative bodies

This case for exemption only applies to investigative bodies who are processing the personal data in respect of a crime. It will apply to the following institutions, as well as to certain others when applicable:

- the police, criminal courts, prisons, non-policing law enforcement; and
- any other body that has statutory functions to exercise public authority or public powers for any of the law enforcement purposes.

In respect of the investigation of a crime, this will include, but is not limited to, the following:

- the prevention, investigation detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

This exemption will not apply to processing that is carried out by an investigative body, but which is not for the primary purpose of investigations into a crime. For example, if a controller is an investigative body it is very likely that they are also processing personal data for general purposes such as for internal HR processes and procedures. This processing is not strictly for law enforcement purposes and so will not fall under this exemption.

When assessing whether this exemption will apply investigative bodies should consider the primary purpose of the processing in question. This should help controllers identify whether the processing constitutes being for the purpose of investigating a crime or not.

## 6. What obligations does each exemption relieve controllers of?

### 6.1. Exemption from Article 4 - Permitted reason for processing

If a controller processes any Personal Data in relation to the above five cases, then it will not need to have a permitted reason for processing such personal data and may proceed to process the data without permitted reason.

The controller should still document processing activities that are exempt from Article 4 within their RoPA.

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

For further information on how to document processing activities please refer to the Guidelines on Records of Processing Activities (RoPAs) for Regulated Entities.

### 6.2. Exemptions from Article 5 (1), (2), (3) and Article 6 - Obligation to comply with some individual rights

If a controller processes any personal data in relation to the above five cases, then it will not need to have to comply with the following individual rights as set out in the PDPPL:

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

The exemption does not apply to individuals' right to request correction of their personal data under Article 5(4) PDPPL.

Controllers should note that where they are exempt from notifying an individual of the processing of their personal data upon request under Article 6, they will still be required to provide privacy information prior to processing under Article 9 unless they have an exemption as a competent authority under Article 19.

For further information on exemptions under Article 18 please refer to the Guidelines on Exemptions Applicable to Competent Authorities (under Article 18) for Competent Authorities.

For further information on individuals' rights under the PDPPL, including complying with the right to request correction, please refer to the Guidelines on Individuals' Rights for Regulated Entities.

## 7. How do exemptions work in practice?

Whether or not organisations can rely on an exemption will depend on (i) whether an organisation is a controller and (ii) whether they are processing personal data in respect of the one of the five cases as set out above.

Exemptions should not routinely be relied upon or applied in a blanket fashion. Controllers must consider each exemption on a case-by-case basis.

If controllers cannot identify an exemption that applies to what they are doing with personal data, they must comply with the PDPPL in its entirety.

Controllers should document exemptions which they apply within their record of personal data processing, against the specific activities to which they are being applied, and in their data privacy notice(s) and data protection policy. This will ensure that controllers can evidence the transparency and accountability principles set out in the PDPPL.

# End of Document