State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

Data Privacy by Design and by Default

PDPPL-02050208E

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-02050205E	Individuals' Rights Guidelines for Regulated Entities (English)
PDPPL-02050209E	Controller and Processor Guidelines for Regulated Entities (English)
PDPPL-02050201E	Principles of Data Privacy Guidelines for Regulated Entities (English)
PDPPL-02050206E	Data Privacy Impact Assessment (DPIA) 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 "Data Privacy by Design and by Default 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

- When controllers collect, store or use personal data, the individuals whose data they are processing may be exposed to risks. It is important that controllers take steps to ensure that the data is handled legally, securely, efficiently and effectively in order to deliver the best possible care.
- The PDPPL requires controllers to put in place "appropriate administrative, technical and financial precautions" to implement the data privacy principles, safeguard individuals' rights and protect their personal data. Such precautions must be proportionate to the risk of serious damage to individuals' privacy or their personal data. This is known as Data Privacy by Design and by Default (DPbDD).
- Data Privacy by Design means that controllers should put data privacy considerations at the heart of the decision making during both the design phase of projects and then throughout the lifecycle.
- Data Privacy by Default means controllers should, by default, minimise the personal data they process and only collect, process, store and make it available to the extent necessary to achieve the limited purposes for which they are processing it.
- Controllers should consider carrying out an exercise to create a record of their processing activities and to identify processes that may pose a risk to individuals and that require appropriate measures to be put in place.
- It is the controller's responsibility to determine what precautions are appropriate to the risk of serious damage, and they should use Data Privacy Impact Assessments (DPIAs) to do so. Controllers should also consider things like risk analysis, organisational policies, and physical and technical precautions.
- Controllers also must take into account additional requirements about the security of their processing – and these also apply to data processors. Controllers' measures must ensure the 'confidentiality, integrity and availability' of their systems and services and the personal data they process within them.
- Controllers also need to ensure that they have appropriate processes in place to test the effectiveness of their measures and undertake any required improvements. Controllers are ultimately accountable for the level of protection they decide to put in place and, in the event of a breach or a complaint, they may be required to notify individuals and the National Cyber Governance and Assurance Affairs of the risk of serious damage due to the decisions they made.

2. Introduction

The PDPPL requires controllers to implement appropriate administrative, technical and financial precautions to protect personal data. These precautions must be proportionate to the risk of serious damage to individuals. This is known as Data Privacy by Design and by Default (DPbDD).

Controllers should integrate privacy into their processing activities and business practices, from the design stage right through the lifecycle, taking a 'privacy-first' approach with any default settings of systems and applications, for example requiring individuals to opt-in not opt-out.

DPIAs and a Record of Personal Data Processing are integral to DPbDD which, in turn, is a key component of any Personal Data Management System.

These guidelines provide information on the requirements of DPbDD and how controllers should implement them, examples of the measures they can take to protect personal data, and how they should determine what measures are appropriate to the risk of processing.

The requirements for DPbDD can be found in Articles 3, 8 and 13 and are explained in more detail below.

3. DPbDD under the PDPPL

Article 3 of the PDPPL says:

"Each individual has a **right to the protection** of their Personal Data…"

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

For more information on individuals' rights, see the Individuals' Rights Guidelines for Regulated Entities.

Appropriate administrative, technical and financial precautions

Article 8(3) of the PDPPL says:

> "The Controller shall: Take **appropriate administrative, technical and financial precautions to protect Personal Data** in accordance with what is determined by the Competent Department.

Article 13 of the PDPPL says:

> "Each of the Controller and the Processor shall **take the precautions necessary** to protect Personal Data against loss, damage, change, disclosure, access thereto, or the inadvertent or illegal use thereof.
>
> Such precautions shall be commensurate with the nature and the importance of the Personal Data intended to be protected.
>
> The Processor shall forthwith notify the Controller of the existence of any breach of the precautions referred to, or where any risk arises threatening Personal Data in any way."

Controllers are required under Articles 8 and 13 to take all appropriate precautions that are necessary to protect personal data. Such precautions should be proportionate to the nature and importance of the personal data being processed. This means that the measures to protect personal data should be balanced against the risk of damage to an individual's privacy or personal data.

Key concepts of DPbDD

Data Privacy by Design is an approach to developing new processes, products, systems and services that involve the processing of personal data. The approach requires controllers to put data privacy considerations at the heart of the decision making during both the design phase of projects and then throughout the lifecycle. This will help to ensure better and more cost-effective protection for individual data privacy.

Data Privacy by Default is an approach to processing personal data that ensures data is processed with the highest data privacy protection *by default*. It incorporates the principles of purpose limitation, storage limitation and, in particular, data minimisation.

It requires controllers to ensure that personal data is automatically protected in any IT system, service, product, and/or business practice so that individuals do not have to take specific action to protect their privacy. The default option for any choice provided to individuals must be data privacy friendly (e.g. using opt-ins, not opt-outs or pre-checked boxes).

Only data which is necessary for each specific purpose of the processing should be gathered unless the individual allows controllers to collect more.

Complying with DPbDD requirements

Controllers are required to put in place appropriate administrative, technical and organisational precautions to protect the personal data that they process. Controllers are responsible for determining what precautions are appropriate and proportionate to the risk that the processing they undertake may cause serious damage to an individual's privacy and / or personal data.

Controllers must embed data privacy into their processing activities and business practices. Data privacy measures should be at the forefront of their decision making when planning or designing processing activities and then subsequently throughout their lifecycle.

Controllers must take steps to ensure that these precautions are effective and keep them under ongoing review.

If controllers use another organisation to process personal data for them, then that organisation is a processor under the PDPPL. They are also obliged to comply with DPbDD requirements.

Article 11(8) requires controllers to confirm that their processors:

- comply with the instructions the controllers give them,
- adopt appropriate precautions to protect Personal Data, and
- consistently maintain compliance with such instructions and the adoption of such precautions.

For more information on using processors, please see Controller and Processor Guidelines for Regulated Entities.

4. What are the foundational principles of privacy by design?

DPbDD is an internationally recognised approach based upon the seven foundational principles of privacy by design developed by the Information and Privacy Commissioner of Ontario.

The principles of privacy by design are different to the principles of data privacy set out in the guidelines on principles (for more information, see Principles of Data Privacy Guidelines for Regulated Entities). These two sets of principles are not meant to overlap but go hand-in-hand with one another.

The principles of privacy by design are:

1. **Proactive not Reactive; Preventative not Remedial:** The Privacy by Design approach should be proactive rather than reactive.
2. **Privacy as the Default:** Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. No action is required on the part of the individual to protect their privacy − it is built into the system, by default.
3. **Privacy Embedded into Design:** Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not an afterthought.
4. **Full Functionality –** Positive-Sum, not Zero-Sum: Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win win" manner, not through a zero-sum approach, where unnecessary trade-offs are made.
5. **End-to-End Security – Lifecycle Protection:** Privacy by Design, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. All data are securely retained, and then securely destroyed at the end of the process, in a timely fashion.
6. **Visibility and Transparency:** Privacy by Design assures all stakeholders that processing activities are operating according to the stated promises and objectives. Its component parts and operations remain visible and transparent, to both users and providers alike.
7. **Respect for User Privacy:** Above all, Privacy by Design requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate privacy notices, and providing user-friendly choices to empower individuals.

If a controller is using processors, the controller should confirm that these processors demonstrate these DPbDD principles as well.

For more information on the use of processors, please see Controller and Processor Guidelines for Regulated Entities.

5. What are key precautions that the PDPPL requires controllers to implement?

Under Article 11 of the PDPPL controllers must implement the following precautions to an appropriate extent balanced against the risk of serious damage that their processing may cause to individuals' privacy or personal data.

- **Personal Data Management System (PDMS):** Article 11(5) requires controllers to put in place a PDMS to manage their PDPPL compliance programme, a key administrative precaution, which must include the ability to report any breaches to individuals and the National Cyber Governance and Assurance Affairs.
- **DPIAs:** Article 11(1) requires controllers to review their privacy protection measures before proceeding with processing. This is done by completing a DPIA and implementing appropriate risk mitigation actions.
- **Individuals' rights and complaints:** Article 11(4) requires controllers to put a system in place to enable individuals to exercise their rights and to manage and investigate complaints about how the controller processes personal data.
- **Individuals' review and control:** Article 11(6) requires controllers to put in place appropriate technologies to enable Individuals to directly access, review and correct their respective Personal Data.
- **Transparency:** Article 9 requires controllers to notify the individual of key information on how and why the controller is processing their personal data prior to processing. This is done through a public privacy notice.
- **Staff training and awareness**: Article 11(3) requires controllers to provide privacy training and awareness to staff that carry out processing in how to protect personal data.
- **Data security:** Article 13 requires controllers to take necessary precautions to protect personal data from loss, damage, modification, disclosure or being illegally or incidentally accessed or used. This includes both technical and physical security measures.
- **Processors:** Article 11(2) requires controllers to identify processors that are responsible for protecting personal data they process on the controller's behalf, and Article 11(8) requires controllers to confirm that the processors comply with their instructions, confirm that the processors adopt appropriate precautions to protect personal data, and regularly assess such compliance and precautions.
- **Assurance of appropriate precautions**: Article 11(7) requires controllers to carry out regular comprehensive audits and reviews on compliance with privacy requirements.

The precautions listed above and set out in Articles 11 and 13 of the PDPPL are necessary but by no means is this list exhaustive. The depth of training or the comprehensiveness of the controller's PDMS, for example, will depend on what personal data they process and how they process it. Ensuring that the controller's precautions meet the bar required to be deemed 'appropriate' may require them to do much more than the above.

The key is that controllers consider privacy issues from the start of any processing activity and adopt appropriate policies and measures that are appropriate to the risk of serious damage.

6. Implementing DPbDD

Controllers must put in place appropriate administrative, technical and financial precautions to implement the privacy principles, safeguard individuals' rights and keep data secure.

These precautions can be functions, processes, controls, systems, procedures, and measures that organisations can implement to promote secure processing and storage of personal data, avoid data breaches, and facilitate compliance with relevant privacy obligations.

There is no standard approach to doing this. What is appropriate will depend on the circumstances of a particular controller's personal data processing.

As stated above, 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.

Controllers should be confident that the measures they identify to protect the personal data being processed are proportionate to the risk of serious damage to the individual's privacy or their personal data. This requires achieving the right balance between appropriate precautionary measures and the risk posed to individuals, taking into account:

- leading practice including state of the art technology;
- the costs of implementation of various protection measures available;
- the nature, scope, context and purposes of processing (the "what," "who," "how" and "why" of processing); and
- the risk of serious damage to individuals.

Controllers should assess measures identified against the potential for serious damage as part of their DPIA. If there is a breach and damage is caused to individuals, controllers are accountable for the precautions they put in place.

For more information on DPIAs, see Data Privacy Impact Assessment (DPIA) Guidelines for Regulated Entities.

How controllers go about implementing suitable precautions depends on their circumstances, for example, who they are, what they are doing, the resources they have available, and the nature of the data they process. Controllers may not always need to have a set of documents and organisational controls in place, although in many circumstances they will be required to have certain documents available concerning their processing.

Administrative Precautions

Administrative precautions are those that relate to the management of their organisation and the way they carry out tasks to deliver privacy. Common examples of administrative precautions include:

- **Management frameworks:** an operating model containing governance and accountabilities, setting out who is responsible for carrying out PDPPL compliance activities.
- **Records of processing:** to provide controllers with a full understanding of the personal data they process.
- **DPIAs:** to review privacy protection measures prior to, and throughout the lifecycle of processing activities.
- **Data privacy policies and procedures:** policies on privacy, DPbDD and individuals' rights among others setting out the processes that must be followed in order to comply with the principles and requirements of the PDPPL.
- **Training and development measures:** to build a culture of data privacy awareness in the controller's organisation and inform staff of their responsibilities. This may include certifications provided by international associations.
- **Transparency measures:** a reader friendly privacy notice that gives individuals control over their data providing information including why and how the controller processes their personal data, their rights and how to exercise them, and who is responsible for data privacy at the organisation.
- **Tools for individuals' control:** to enable them to determine how the controller is using their personal data, and whether the controller is properly enforcing their policies.
- **Offering strong privacy defaults:** offering strong privacy defaults, user-friendly options and controls, and respect user preferences.
- **Putting contractual requirements on third party processors:** requesting evidence of processors' privacy maturity, including such considerations in the controller's selection process, and putting contracts or written agreements in place that include audit or review measures and instructions for processors on how to protect personal data. For more information about contractual requirements, please refer to the Controller and Processor Guidelines for Regulated Entities.
- **Information security policies and procedures:** covering
    - information security responsibilities;
    - access to premises and / or equipment;
    - business continuity arrangements that identify how the controller will protect and recover any personal data they hold; and
    - periodic checks to ensure that their security measures remain appropriate and up to date.

Technical Precautions

Technical precautions are those that relate to the use of technology to carry out tasks or achieve certain outcomes to deliver privacy. Common examples of technical precautions include:

- **Pseudonymisation and encryption:** using pseudonymisation (replacing personally identifiable material with artificial identifiers) and encryption (encoding messages so only those authorised can read them).
- **Access and retention controls:** to ensure compliance with data minimisation, purpose limitation and storage limitation.
- **Technology for individuals' control:** technologies to enable Individuals to directly access, review and correct their respective personal data.
- **Physical security measures:**
    - the quality of doors and locks, alarms or CCTV;
    - how the controller controls access to their premises, and how visitors are supervised;
    - how the controller disposes of any paper and electronic waste; and
    - how the controller keeps IT equipment, particularly mobile devices, secure.
- **Cybersecurity measures:**
    - system security – the security of the controller's network and information systems, including those which process personal data;
    - data security – the security of the data the controller holds within their systems, e.g. ensuring appropriate access controls are in place and that data is held securely;
    - online security – e.g. the security of the controller's website and any other online service or application that they use; and
    - device security – including policies on Bring-your-own-Device (BYOD) if the controller offers it.

What technical precautions are appropriate will develop and change over time as technology develops and as such, we cannot give specific guidance on particular technologies. Controllers will need to include such considerations in their information security risk assessments and DPIAs.

Financial Precautions

Financial precautions are those that relate to investment in products or services to carry out tasks or achieve certain outcomes to deliver privacy. Such investment could be in relation to implementing administrative or technical precautions. Common examples of financial precautions include:

- **investment in technology:** to provide individuals with control over their personal data, to keep their data secure or to support the organisation with your compliance programme;

- **investment in professional advice:** to obtain specialist privacy or information security advice that goes beyond the scope of these guidelines; and
- **allocation of a budget for privacy compliance:** to undertake privacy compliance activities to comply with the PDPPL or international best practice.

Determination of appropriate precautions

Some precautions that controllers put in place will be enterprise-wide and others will only be applicable to specific processing activities.

Controllers' precautions must protect personal data by:

- 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.

Controllers must assess the appropriateness of their precautions using a DPIA considering the following:

- their precautions need to be appropriate to the size of their organisation and use of their network and information systems;
- they should take into account the state of technological development, but they are also able to consider the costs of implementation;
- their precautions must be appropriate to their business practices. For example, if they offer staff the ability to work from home, they need to put measures in place to ensure that this does not compromise privacy; and
- their precautions must be appropriate to the nature of the personal data they hold and the serious damage that might result from any compromise.

In assessing the appropriate precautions, account should be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Successful privacy compliance programmes are united behind a common vision and employ a holistic, multidisciplinary approach bringing together expertise from legal, security, risk and data privacy teams with representatives from across the business who have a deep understanding of how the organisation processes personal data. It is important that controllers include people in their assessment process with the required expertise to support their judgement of what constitutes 'appropriate.'

Controllers may also wish to leverage the expertise of service providers who are accredited against national standards for information security and/or privacy to support their programmes such as the NISCF.

Key information controllers should use in supporting their deliberations regarding appropriate measures include:

- related pieces of the legislative framework that contain security provisions, such as the National Information Assurance Policy and Cloud Security Policy;

- the output of regulatory institutions, such as the Communications Regulatory Authority for the telecom sector;
- the output of information security centres of excellence, such as Q-CERT;
- policy frameworks of national governments, such as national privacy and cybersecurity plans;
- regulatory policy statements and other guidance issued by the national privacy regulators and by sector regulators;
- decisions in regulatory enforcement actions brought by the national privacy regulators and related regulators;
- decisions of courts and tribunals in related areas;
- national and international standards for best practice, such as the Qatar National Information Assurance Policy, any accreditations or certifications issued by the National Cyber Governance and Assurance Affairs, the ISO 27000 series, the Payment Card Industry Data Security Standard, CBEST and the NIST framework;
- threat assessment reports and subject matter white papers published by IT security and privacy companies and consultants; and
- the output of relevant professional associations and affinity groups. There are many operating in the space, such as the International Association of Privacy Professionals, the Cloud Security Alliance and the Information Security Forum.

This list is not exhaustive but provides examples of the range of available resources in determining what precautions are appropriate.

Controllers must document the considerations they made in assessing the risk of serious damage, the available precautions and their appropriateness.

For more information on DPIAs, see the Data Privacy Impact Assessment (DPIA) Guidelines for Regulated Entities.

End of Document