State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

Privacy Notice

PDPPL-02050213E

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)

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 "Privacy Notice 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 purpose of these guidelines is to explain the requirements placed on Controllers to comply with Article 6 of the PDPPL regarding individuals' right to be notified and Article 9 regarding the information which must be provided to individuals prior to processing.
- Controllers must provide individuals with 'privacy information' including:
    - details of their organisation,
    - a description of how personal data is processed,
    - the permitted reasons and purposes for processing,
    - how long personal data is retained for and
    - who it will be shared with as well as other necessary information set out in these guidelines.
- Controllers must provide privacy information to individuals before or at the time they collect their personal data from them.
- If controllers obtain personal data from other sources, they must provide individuals with privacy information within a reasonable period of obtaining the data and no later than one month.
- Privacy information is usually provided via a privacy notice which is a key document that controllers must put in place if they collect, use or process personal data in any way.
- The provision of comprehensive and transparent privacy information provides individuals with control and choice over their personal data and privacy.
- There are specific requirements that controllers must consider in respect to preparing privacy notices directed at children when operating child-based websites.
- There is an exemption for competent authorities from the requirement to provide a privacy notice under Article 9 when they are processing personal data for specific reasons listed in Article 18.

2. Introduction

The PDPPL requires controllers to provide privacy information to individuals about the way they intend to process individuals' personal data prior to processing. Articles 6(1) and 9 of the PDPPL set out requirements regarding the information that should be provided.

Privacy information should be provided to individuals in a publicly-available privacy notice enabling them to understand key information about the processing the controller will undertake. These guidelines set out the obligations of controllers in more detail and have been developed to support them in preparing their privacy information and developing their privacy notice.

The approach controllers take should be based on their specific organisational circumstances as they know their organisation best. Controllers should be confident that they can justify the approach they take to their privacy notice in line with the principle of accountability.

3. What does the PDPPL say about the information to be provided to individuals?

Article 9 of the PDPPL says:

> *"The Controller shall, prior to starting to process any Personal Data, inform the Individual with the following:*
>
> 1. *The Controller's details or any other party conducting the processing for the Controller or to be used thereby.*
> 2. *The Lawful Purposes that the Controller or any other party wants to process the Personal Data therefor.*
> 3. *Comprehensive and accurate description of the processing activities and the levels of disclosure of such Personal Data for the Lawful Purposes, and if the Controller fails to do so, the Controller shall provide the Individual with a general description thereof.*
> 4. *Any other information that is necessary and required for fulfilling conditions of Personal Data Processing."*

Article 9 places obligations on the controller to provide information to the individual prior to processing their personal data and is in line with the principle of transparency as set out in Article 3 of the PDPPL. Transparency is the idea that personal data must be processed in a clear, open and honest way.

The information that controllers must provide to individuals includes:

Article 9(1)

- Details about the controller
- Details about any third-party processors

Article 9(2)

- The lawful purposes for processing
- The lawful purposes of any third-party processors

Article 9(3)

- A comprehensive and accurate description of the processing activities
- The levels of disclosure for the lawful purposes or a general description

Article 9(4)

- Any other information that is necessary and required for fulfilling conditions of personal data processing.

Each of these legal requirements is dealt with in more detail below.

4. What is a privacy notice?

A privacy notice is a public-facing document through which controllers formally notify individuals that they are processing personal data and provide these individuals with privacy information in a clear, open and honest way. It enables individuals to understand how their personal data is being processed and exercise their rights under the PDPPL.

Why is a privacy notice important?

Being open and upfront about what they do with personal data helps controllers to deal with individuals in a clear and transparent way, providing them with control over their personal data and their privacy. Privacy notices are often the first impression given to individuals regarding how organisations treat their personal data and privacy. High quality privacy notices serve to build public confidence, enabling organisations to distinguish themselves from their competitors.

What are the possible consequences of not providing a sufficient privacy notice?

If controllers do not provide sufficient and transparent information to individuals, they could be liable to fines under Article 23. They may also suffer reputational damage for getting it wrong. If controllers are not honest with people about what they do with their data, or if controllers hide important information behind overly complex and legalistic language, individuals may be less willing to put their trust in controllers and provide their personal data.

5. What must a privacy notice include in brief?

A privacy notice must include the privacy information required under Articles 6(1) and 9 of the PDPPL. The table below details what information is necessary for controllers to provide:

Article	Requirement	In practice
Article 9(1)	Details about the controller	• **(Always)** The legal name of the controller • **(Always)** A description of the controller • **(Always)** The registered address of the controller • **(Always)** Contact information for the controller • **(If applicable)** Contact information for the person or team responsible for data privacy
	Details about any third-party processors	• **(If applicable)** The name or categories of any processors or joint controllers the controller uses • **(If applicable)** A general description of why they process personal data with the controller or on the controllers behalf • **(If applicable)** Their geographic location
Article 9(2)	The permitted reasons for processing	• **(Always)** The controller's purposes for processing including the permitted reasons, whether this is consent or a lawful purpose (legitimate interest, legal obligation, contractual obligation) • **(If applicable)** A description of the controller's legitimate interests where legitimate interest is the permitted reason for processing
	The permitted reasons of any third-party processors	• **(If applicable)** The permitted reason for processing, whether this is consent or a lawful purpose (legitimate interest, legal obligation, contractual obligation), of any processors or joint controllers that the controller uses.
Article 9 (3)	A comprehensive and accurate description of the processing activities	• **(Always)** What personal data is processed highlighting where such data is of a special nature • **(Always)** How personal data is collected • **(If applicable)** Third parties that personal data is

	The levels of disclosure for the permitted reasons or a general description	shared with or a general description of such third parties • **(Always)** The length of time personal data is retained for • **(If applicable)** The details of whether individuals are under a legal or contractual obligation to provide personal data and the consequences of not complying with such an obligation

Article 9(4)	Any other information that is necessary and required for fulfilling conditions of personal data processing.	• **(Always)** General information on how personal data is kept secure
		• **(Always)** Individuals' rights under the PDPPL and how they may exercise them
		• **(Always)** Individuals' right to make a complaint to the National Cyber Governance and Assurance Affairs.
		• **(If applicable)** Details of any Cross-Border Data Flows that the controller is undertaking including:
		  ○ the locations that personal data is being transferred to
		  ○ the safeguards in place to protect individuals' personal data and privacy.
		• **(If applicable)** Details of any automated decision-making, including profiling.

6. What must a privacy notice include in more detail?

The PDPPL specifies what controllers need to tell individuals when they collect personal data. There are some types of information that must always be provided and others that only need be provided in certain circumstances.

Controllers are accountable for how they process personal data and for doing so transparently by providing the necessary privacy information to individuals. They are also obligated to give individuals control over their personal data by enabling them to exercise their rights when they wish to do so.

The table below explains what privacy information controllers need to include when drafting their privacy notices and under what circumstances.

6.1. Details about the Controller

Controllers must provide information about their organisation so individuals can easily understand who they are, what they do, where they are located and how to contact them.

What information must be provided?	How should this information be provided and why?
The legal name of the controller.	Controllers must provide the legal name of their organisation. E.g. *"This privacy notice sets out how [Example Company Limited.] processes your personal data..."* This provides individuals with clarity as to the entity that is legally responsible for processing their personal data.
A description of the organization.	Controllers must provide a description of their business and its purpose for operating. E.g. *"[Example Company] is a [Qatari airline / hospitality group / etc] that [provides airline travel / accommodation services / etc.]."* This provides individuals with the context in which the controller processes their personal data.
The legal address of the business.	Controllers must provide the registered address of the organisation. E.g. *"[Example Company] is registered at [full address]"* This provides individuals with an understanding of where you are based so that they can understand which laws may apply to you.
Contact information for the controller.	Controllers must provide the contact information for the organisation. E.g. *"If you wish to contact us, or want more details about how we use your personal data, you can call us on 4000 0000*

	(+974 4000 0000 from outside the State of Qatar) or contact us using the following [email / webform / etc.]" This enables individuals to contact you with any query related to your organisation and to data privacy in particular, if the controller does not have a dedicated privacy team.
Contact information for the person or team responsible for data privacy.	If controllers have a dedicated staff member or team responsible for data privacy and / or PDPPL compliance, they should provide individuals with a way to contact them. E.g. *"To contact our [Data Protection Officer / Data Privacy Team / person responsible for data privacy / etc.] you can send an email to privacyemailaddress@examplecompany.qr"* This enables individuals to contact the team responsible for data privacy with any privacy related queries.

6.2. Details about any third-party processors

Controllers must provide information about any processors or joint-controllers they use so individuals can easily understand who the controller shares their personal data with, what the third party does, where they are located and how to find out further information about them and how they might process individuals' personal data.

What information must we provide?	What exactly is the information we need to include?
(If applicable) The name or categories of any processors or joint controllers the controller uses.	Controllers must provide the name or categories of any processors or joint controllers that they process personal data with or who process it on their behalf. This provides individuals with clarity as to the organisations that the controller shares their personal data with to process their personal data with or on behalf of the controller.
(If applicable) A general description of why they process personal data with the controller or on their behalf.	Controllers must provide a general description of why processors and joint controllers process personal data with them or on their behalf. *E.g. "[Example Processor] is a [recruitment company / travel group / etc.] that processes personal data on our behalf to [identify candidates for employment / make accommodation bookings for our customers / etc.]"* This provides individuals with the reasons why the controller uses third parties to process personal data for them.

(If applicable) Their geographic location.	Controllers must provide the location of any processors or joint controllers. E.g. "*[Example Processor] is located in [London, United Kingdom / etc.]*" This provides individuals with an understanding of where organisations are based that process personal data with the controller or on their behalf.

6.3. The permitted reasons for processing

Controllers must provide information about their permitted reasons for processing and, when relying on consent or legitimate interests, detailed information so that individuals can understand the judgements controllers have made in relation to their privacy and personal data and exercise their rights under the PDPPL if they wish.

What information must we provide?	What exactly is the information we need to include?
(Always) The controller's purposes for processing including the permitted reasons, whether this is consent or a lawful purpose (legitimate interest, legal obligation, contractual obligation).	Controllers should explain why they use individuals' personal data. They should be clear about each different purpose for processing. There are many different reasons for using personal data and controllers will know best the particular reasons that they process personal data for. Common purposes could include marketing, order or transaction processing, and/or staff administration. Controllers should provide the permitted reason for processing they are relying on in order to collect and use individuals' personal data. This will be consent or one of the lawful purposes.
(If applicable) A description of the controller's legitimate interests where legitimate interest is the permitted reason for processing.	Controllers should set out the legitimate interests that they rely on where they are relying on legitimate interest as a permitted reason for processing. This provides individuals with an understanding of how controllers balance the legitimate interests of the controller against individuals' privacy.

6.4. The permitted reasons of any third-party processors

Controllers must provide information about the permitted reasons for processing that any processors or joint controllers that the controller uses are relying on. This ensures individuals have a full view of the permitted reasons being relied on by all parties using the personal data that the controller obtains.

What information must we provide?	What exactly is the information we need to include?
(If applicable) The permitted reason for processing, whether this is consent or a lawful purpose (legitimate interest, legal obligation, contractual obligation), of any processors or joint controllers that the controller uses.	Controllers should explain why third parties use individuals' personal data on the controller's behalf. They should be clear about each different purpose for processing. They should provide the permitted reason for processing that the third parties rely on in order to collect and use individuals' personal data. This will be consent or one of the lawful purposes (legitimate interest, legal obligation, contractual obligation).

6.5. A description of the processing activities, levels of disclosure or a general description of the levels of disclosure.

Controllers must provide individuals with comprehensive information about their personal data processing activities and the organisations they share personal data with. Such information provides individuals with an understanding of how controllers process their personal data to inform the choices individuals make when exercising control over their personal data.

What information must we provide?	What exactly is the information we need to include?
(Always) What personal data is processed, in particular personal data of a special nature.	Controllers must provide individuals with information regarding what personal data they process, in particular setting out any personal data of a special nature that they use.
(Always) How personal data is collected.	Controllers must inform individuals of the source of the personal data. They should tell individuals where they obtained their information, and if it was obtained from a publicly accessible source, they must make this clear. When providing this information controllers should be as specific as possible and name the individual source(s) the personal data was obtained from. If this is not possible then they should provide more general

	information, for example using descriptions of the methods of collection.
(If applicable) Third parties that personal data is shared with or a general description of such third parties.	Controllers must provide individuals with the details of anyone that processes the personal data on their behalf, as well as all other organisations. They should provide individuals with the names of the organisations or the categories that such organisations fall within. If only telling individuals the categories of organisations, controllers should be as specific as possible.
(Always) The length of time personal data is retained for	Controllers must tell individuals for how long they will keep their personal data. If controllers do not have a specific retention period, then they should inform individuals of the criteria used to decide how long the information will be kept. Common examples of such criteria include for compliance with a legal obligation, for operational reasons, or for crime prevention purposes.
(If applicable) The details of whether individuals are under a legal or contractual obligation to provide personal data and the consequences of not complying with such an obligation.	Controllers must inform individuals if they are required by law, or under contract, to provide personal data to them, and what will happen if they do not provide that data. For example, they could be in violation of a law, or they may not be able to proceed with the contract. This will often only apply to some, and not all, of the information being collected, and controllers should make it clear to individuals about the specific types of personal data that are required under a legal or contractual obligation.

6.6. Any other information that is necessary and required for fulfilling conditions of personal data processing

Controllers must provide individuals with further necessary information relating to the personal data they hold. Such information informs individuals of how to exercise their rights, how the controller protects their personal data and highlights any transfers of personal data to locations where the PDPPL does not apply.

What information must we provide?	What exactly is the information we need to include?
(Always) General information on how personal	Controllers must provide details of the security measures in place to protect the personal data that they hold.

data is kept secure.	*Examples of such measures may include access control, encryption, disposal methods, etc.*
(Always) Individuals' rights under the PDPPL and how they may exercise them.	Controllers must inform individuals which rights they have under the PDPPL in relation to the use of their personal data, for example: • the right to withdraw consent where applicable; • the right to object to processing in certain circumstances; • the right to erasure; • the right to request correction; • the right to be notified of inaccurate disclosure; • and the right to access.
(Always) Individuals' right to make a complaint to the National Cyber Governance and Assurance Affairs.	Controllers must inform individuals of their right to make a complaint to the National Cyber Governance and Assurance Affairs. Controllers should provide the name and contact details of the National Cyber Governance and Assurance Affairs.
(If applicable) Details of any Cross-Border Data Flows that the controller is undertaking.	Controllers must inform individuals of the transfer of their personal data to any countries or organisations outside of the State of Qatar. This must include: • the locations the personal data is being transferred to • brief information on the safeguards in place to protect individuals' personal data and privacy.
(If applicable) Details of any automated decision-making, including profiling.	Controllers must inform individuals if they are making decisions based solely on automated processing, including profiling, that have legal or similarly significant effects on individuals. Meaningful information about the logic involved in the process and an explanation of the significance and envisaged consequences should be included.

7. How must controllers provide individuals with privacy information?

7.1. When should privacy information be provided?

Controllers must provide privacy information to individuals prior to processing personal data. This means that it should be provided before or at the point of first collection or processing of the personal data when personal data is obtained from a source other than the individual it relates to, it may not be practical to provide this information at the time of collection or beforehand so controllers must provide the individual with privacy information:

- within a reasonable period of obtaining the personal data and no later than one month after collection;
- if there are plans to communicate with the individual, at the minimum share the privacy information no later than when this first communication takes place; and
- if there are plans to disclose the personal data to another party, the privacy information should be provided no later than when such disclosure is made.

Controllers must be proactive in providing privacy information to individuals. They can meet privacy information requirements by putting the information on their website but must also make efforts to inform individuals of its existence and location.

This means that controllers are required to provide a link to their privacy notice in any communication with individuals and should make sure that they have communicated the location of their privacy notice directly, for example by email, text message or as part of an information collection form, to the individual no later than the first communication or one month after collection.

7.2. Where should privacy information be provided?

Privacy information should be provided at the point of collection of the personal data and should be transparent, publicly available and easily accessible.

- **Where personal data is collected from an individual online:** privacy information should be provided, for example, by providing a pop-up notice which sets out the information at a high level and provides a link to a full privacy notice. It is not enough for the controller to post their privacy notice on their website and not direct individuals to it.
- **Where personal data is collected from an individual physically or in person via traditional offline methods:** privacy information should be provided, for example, by posting a hard copy privacy notice at the premises where individuals can easily read it or by including the notice on the form by which the individual provides their personal data.

7.3. What are the exemptions from providing a privacy notice?

Controllers must provide privacy information to individuals prior to processing their personal data unless they are exempt from doing so under Article 18 as competent authorities where they process personal data for specific purposes.

For more information on the exemptions for competent authorities under Article 18 please see Competent Authority Exemptions Guidelines for Regulated Entities.

8. How do controllers put a privacy notice in place?

Much of the information that controllers require in order to draft their privacy notice may be gathered whilst preparing a Record of Processing Activities (RoPA) which forms the backbone of a controller's data privacy compliance programme and contains information about how they process personal data.

Further relevant information on specific processing activities may also be held in records of Data Protection Impact Assessments (DPIAs). Both RoPA and DPIA are key inputs into a controller's privacy notice and should be undertaken to ensure their privacy notice is based on a full and comprehensive understanding of the processing taking place.

8.1. What are the key characteristics of an adequate and appropriate privacy notice?

For a privacy notice to be effective in providing the privacy information required under Article 9, it must be provided in compliance with the principle of transparency, honesty and respect for human dignity. This means it must be written and presented in a way that is engaging, easily understandable and appropriate for the target audience.

In terms of writing style and sequence, an appropriate and effective privacy notice is:

- **concise:** keeping sentences short and to the point by including only relevant information whilst using headings to break up the notice and signpost the reader.
- **transparent:** clearly and actively drawing the reader's attention to any use of their personal data that may be unexpected or have a significant impact on them and providing clear specific choices that are not misleading or counterintuitive.
- **intelligible:** using language that is precise, unambiguous and understandable to the individuals whose personal data is being collected and processed, explaining complex matters in plain and simple terms.
- **easily accessible:** provided in a place that is easy for individuals to find, apart from other information (such as terms and conditions), relevant to the context in which personal data is collected and consistently accessible across multiple platforms.
- **uses clear and plain language:** using common, straightforward everyday words and phrases that are familiar to individuals whilst avoiding confusing terminology, jargon, or legalistic language.

The controller is accountable for ensuring that it meets the above characteristics for being adequate and appropriate. Privacy notices should be written in the languages through which the controller provides its services and / or products so that it is intelligible to its customers. For example, if forms to open an account, communications or products are provided in Arabic, the controller should have an Arabic privacy notice. If the controller also provides forms, communications or products in English, they should also have an English privacy notice.

8.2. What medium should controllers provide their privacy information through?

In terms of presentation and delivery, an appropriate and effective privacy notice may be provided:

- **verbally:** face-to-face or over the phone, for example when collecting information verbally for an agent to complete a form.
- **in writing:** through printed media or included as part of a form that is used to collect personal data.
- **through signage:** through signs on the walls of premises, for example informing individuals that CCTV is being used to keep the premises secure.
- **electronically:** using electronic communications or platforms for example text messages; on websites; emails or through mobile apps.

The most easily accessible way for a controller to deliver privacy information is often to use the same medium through which they collect the personal data. A blended approach uses a combination of techniques to provide privacy information in the most easily digestible form.

8.3. What techniques should controllers consider when providing their privacy information?

Controllers should consider incorporating a variety of techniques taking advantage of all of the technologies available to them. Depending on controllers' circumstances, techniques they may use include:

- **a layered approach:** providing key privacy information immediately and having more detailed information available elsewhere for those that want it, for example through a drop-down section or via a link. This approach enables controllers to provide an easily navigable document whilst needing to explain complicated information to people;
- **dashboards:** providing individuals with preference management tools that can give individuals hassle-free control over their personal data allowing them to alter settings, for example revoking consent or changing cookie preferences;
- **just-in-time notices:** providing individuals at the time they provide personal data with a brief message containing specific information on how their data will be used; for example using pop-up boxes or hover over features with further layers of information available; and
- **icons:** complementing written privacy information with icons to support individuals in understanding and digesting the information.

The most effective privacy notices are useful, engaging and designed with the individual in mind. Controllers should use a multi-disciplinary team including legal, communications, marketing, IT and customer service expertise when developing their privacy notice.

Privacy notices are a key obligation for controllers under the PDPPL. They are also an opportunity to build a relationship of trust with individuals, developing the controller's image and complementing their brand and reputation.

9. What process could controllers follow to develop their privacy notice?

Controllers should take a methodical approach to preparing their privacy information in order to be sure that they have included the required information and presented it in an appropriate way. Controllers may wish to consider including the following activities in their approach to developing their privacy notice:

1. **Confirm privacy information:** Reviewing their data processing documentation to ensure they have the necessary information to include in the privacy notice, this will often be captured in their RoPA and DPIAs but may be captured elsewhere.
2. **Identify stakeholders:** Identifying key stakeholders in departments that are likely to have skills relevant to drafting privacy information but also presenting it in a user-centric and easily accessible way.
3. **Draft privacy notice:** Document privacy information in a privacy notice and ensure the correct information is included in a clear and concise manner.
4. **Design privacy notice and methods:** Design the privacy notice and other related techniques for providing privacy information to individuals, for example just-in-time notices, including how, where and when they will be presented to individuals.
5. **Test privacy notice on individuals:** Gather user feedback from individuals who the privacy notice is targeted at and incorporate suggestions to make it as user-friendly as possible.
6. **Ongoing review:** Keep privacy notices under regular review to ensure that they are accurate and up to date, taking account of any changes to the way personal data is processed.

10. What are the specific requirements when operating a website addressing children?

The personal data of children is regarded as personal data of a special nature under Article 15 of the PDPPL. It requires a higher level of protection due to its sensitivity.

Controllers who own or operate websites addressing children have specific additional obligations under Article 17. This is because children are less likely to be aware of the potential risks involved when their personal data is processed.

10.1. What does the PDPPL say about the information to be provided to children?

Article 17 of the PDPPL says:

> *''...an owner or operator of any website addressing children shall take into account the following:*
>
> 1. *Posting a notification on the website as to what child data is, the way of its use, and the policies followed in the disclosure thereof."*

10.2. What privacy information must controllers provide to children?

Controllers must provide children with the same information as they would give to adults as set out above. The requirements for transparency and providing individuals with control and choice apply to children.

In addition, controllers must provide information specifically and separately about:

- what personal data of children they will process;
- the way they will process it; and,
- information about the policies they use to make decisions regarding how and when they disclose children's personal data to third parties.

Privacy notices relating to children should be:

- **Age-appropriate:** The language must be understandable by children of the age that it relates to. If processing relates to both teenagers and young children for example, controllers should consider separate notices aimed at each age range.
- **Appealing:** Controllers should present their privacy notice(s) in a way that is appealing to a young audience. They may consider using diagrams, cartoons, graphics, symbols and other methods that will attract and interest them.

10.3. What does the PDPPL say about information to be provided to guardians?

Article 17 of the PDPPL says:

> *''...an owner or operator of any website addressing children shall take into account the following:*
>
> 2. *Obtaining, either electronically or through any other appropriate means, an explicit consent from the guardian of the child whose Personal Data is processed.*

3. *Providing a child's guardian, upon the request thereof, and after verifying the identity thereof, with a description of the type of the Personal Data processed, along with stating the purpose of the process together with a copy of the data processed or gathered about the child.*
4. *Deleting, removing or suspending processing any Personal Data that has been gathered from or about a child, if such is requested by a child's guardian. "*

10.4. What privacy information must controllers provide to guardians?

Controllers must provide guardians with information about how to exercise control and choice on behalf of their child(ren). This should include information on:

- the process for guardians to provide consent for processing on behalf of the child and how this consent may be withdrawn by either the guardian or the child.
- the process for verifying the identity of the guardian and their relationship to the child in order to enable the guardian to exercise the child's right to:
    - be notified upon request with a description of the personal data being processed, the permitted reasons and purposes for processing being relied on and obtain a copy of the data being processed.
    - have their personal data deleted or removed in line with the right to erasure.
    - have the processing of their personal data suspended in line with the right to object.

End of Document