State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

Electronic Communications for Direct Marketing

PDPPL-02050218E

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-02050213E	Privacy Notice Guidelines for Regulated Entities (English)
PDPPL-02050209E	Controller and Processor 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 "Electronic Communications for Direct Marketing 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

- Direct marketing is the communication of advertising or marketing material directly to individuals. It is largely carried out by controllers via electronic means.
- Controllers should not send direct marketing communications to individuals unless they have obtained their explicit consent for such direct marketing. Individuals must also be able to withdraw their consent. Such consent must be:
    - **Explicit and unambiguous:** Controllers should ensure that individuals are well informed about what they are providing their consent for, by including an appropriate consent notice on the particular web page or form that collects their consent. This information should also be reflected in the controller's privacy notice.
    - **Opt-in and not opt-out:** Individuals should provide their consent through a clear affirmative action. Indirect consent such as via pre-ticked boxes or first seeking consent via opt-out notices in the first marketing communication will not be lawful.
    - **Easy to withdraw:** Controllers should ensure that the individuals are aware of the means through which they can withdraw their consent and thus stop receiving direct marketing messages from the controller unless they provide their explicit consent to receive such marketing again.
- Direct marketing communications should clearly identify the controller and the controller's contact information to the individual in case the individual wishes to stop receiving further direct marketing communications i.e. withdraw their consent.
- Controllers should not buy email lists or any list (whether anonymised or not) of contact information of individuals to send direct marketing communications to. Controllers should also exercise caution in engaging with a third party to market to individuals on the controller's behalf.

2. Introduction

In order to promote their organisation or its products or services, controllers may elect to send advertising or marketing material electronically to particular individuals that is directly addressed to them using their personal data. This practice is known as direct marketing.

These guidelines have been prepared by the National Cyber Governance and Assurance Affairs to provide controllers with information on what constitutes electronic communications and direct marketing and what they should do if they plan to process personal data in order to carry out such communications. The requirements for electronic communication for the purpose of direct marketing can be found in Article 22 and are explained in more detail below.

3. What is direct marketing?

Article 1 of the PDPPL says that:

- Direct Marketing means "sending any advertising or marketing material, in whatsoever means, to certain individuals."
- Electronic Communication means "a communication by means of any of Wire and Wireless Communications."

Direct marketing involves the communication, by whatever means, of any advertising or marketing material which is directed to particular individuals.

In today's world, direct marketing occurs almost entirely via electronic communications (e.g. email, text messaging or social media) to individuals. Marketing mail that is delivered in hard copy to an individual's physical address is not covered by the Article 22 requirements of the PDPPL. Best practice, however, would involve controllers applying the same requirements to their hard copy direct marketing as they do to their direct marketing via electronic communications.

Even where controllers are processing personal data for non-electronic direct marketing and such processing is not covered by Article 22 requirements, they must still comply with all other obligations in respect of the PDPPL in regards to this processing.

4. What does the PDPPL say about direct marketing and electronic communication?

Article 22 of the PDPPL says:

> "No Electronic Communication shall be made with individuals for Direct Marketing **without obtaining such Individual's prior consent**.
>
> In case the aforesaid consent is given, the electronic message **shall include identity of sender** with an explicit notice indicating that the **purpose of such message is Direct Marketing**. In addition, the message shall include a valid address for easy access as **through which individuals can send a request** to sender **to stop or unsubscribe from such messages**."

In summary, the PDPPL says the following about electronic communications for direct marketing:

- Controllers should not send direct marketing messages electronically to individuals unless they have received consent from the individual for this purpose, in accordance with the permitted reason for processing the personal data.
- The controller should include its identity and the purpose of processing (direct marketing) unambiguously in the direct marketing communication sent to the individuals.
- Individuals can, at any time, withdraw their consent i.e. request to stop receiving direct marketing messages even for which they had provided their consent earlier. Such a request has to be fulfilled by the controller in a way that these individuals will not receive direct marketing messages unless they provide their consent once again. Controllers must not make it difficult for individuals to withdraw their consent.

5. PDPPL requirements around direct marketing in more detail

5.1. The requirement to obtain explicit consent before processing

The PDPPL requires that controllers send any electronic communication for the purpose of direct marketing to individuals only after obtaining the individual's consent for such direct marketing communications. This means that consent is the only permitted reason for processing any direct marketing related processing activity.

What is unambiguous consent?

For any processing activity that relies on consent as a permitted reason, controllers should ensure that the consent collected from the individual is unambiguous, i.e. a reasonable individual should know what they are consenting to. Consent requests cannot be merged with other terms and conditions and must be via a very clear statement.

What is the difference between opt-in and opt-out?

Consent should be provided by the individual as an affirmative positive action, i.e. not through pre-ticked boxes or "implicit" consent that can be inferred from the individuals' actions, it instead requires a positive opt-in.

Examples:

- Controllers may use "cookies" on the individual's web browser to target direct advertisements messages towards the individual. Such cookies should be deployed only after the individual has "opted-in" i.e. has "clicked accept" to allow such direct marketing cookies to be deployed on the individual's browser. Controllers cannot deploy such cookies (which are not necessary for the functioning of the controller's website or web application) on the individual's browser by serving a short privacy statement and relying on the individual's "implicit consent" and allowing them to "opt out" of such a processing activity.
- Controllers may collect individuals' email addresses on a web page of the controller's website. The controller must make it clear, on the web page, that if the individual provides their email address in that instance, they are providing their consent towards receiving direct marketing emails until they withdraw their consent. The controller makes this clear via a "consent notice" above the input field for the individual's email ID and the "submit" button. This shows that the individual is providing their consent unambiguously as an affirmative positive action. If there is a pre-ticked box stating that the individual "accepts terms and conditions", this will be too ambiguous and is considered "opt-out" and not "opt-in".

Should controllers keep evidence of consent?

Controllers must keep a record (evidence) of consent to be able to demonstrate that they have received the individual's unambiguous consent via the individual's affirmative action. Such evidence should ideally include the timestamp of the individual's affirmative action. The controller could also include the location of where the individual provided their unambiguous consent, however the controller should be wary of processing location related data and ensure it adopts data privacy by design in designing and implementing any processing activity.

What are the other provisions for relying on consent that controllers should consider before processing?

- Controllers cannot collect a "blanket" consent for more than one processing activity. For example, in collecting the individual's consent, controllers cannot use it for "any or all future direct marketing communications". Each consent must be for a specific direct marketing channel.
- Controllers cannot make consent to processing personal data a prerequisite for offering goods and services. For example, controllers cannot offer a discount on its goods or services to individuals on the condition that the individual provides their consent towards receiving direct marketing communication.
- Controllers must name any third-party controllers who will rely on the consent. For example, if the controller uses any processors to execute such direct marketing, the controller must state the name of this processor in their privacy notice.
- Controllers cannot rely on consent to process personal data of their employees to execute their obligations as an employer, as it is difficult to legitimately prove that they received their employee's consent freely.
- The controller's privacy notice needs to be updated to reflect this processing activity and consent as its permitted reason. For more information on privacy notices, please refer to the Privacy Notice Guidelines.

5.2. The requirement to include the identity of the originator

The PDPPL requires that any direct marketing message includes "the identity of the originator". While the "originator" is not defined in the law, in this context it can be interpreted as the party sending the direct marketing communications. This means that the originator is the controller, unless the controller uses a third party to send direct marketing messages on its behalf.

How do we include the identity of the originator?

There are many ways to include the identity of the originator in direct marketing communications. It depends on the channel of communication. Examples are given below.

If the direct marketing is via email, the controller should ensure:

- the email ID from which the individual receives the direct marketing communications is not misleading and the name of the originator is clearly stated i.e. the organisation that the communication has been sent on behalf of;
- the email clearly and obviously states that it has been sent for the purpose of direct marketing including appropriate reference to the consent that the individual has provided;
- the email contains contact details of the originator which the individual can use to opt out of future communications or revoke their consent for receiving direct marketing;
- the email contains a link to the controller's privacy notice; and

- consideration is given to whether their proposed communication constitutes spam.

N.B. Controllers should also review any anti-spam guidelines issued by the Qatari National Cyber Security Agency (NCSA) or other bodies.

If the direct marketing is via text message, the controller should ensure:

- the name of the sender of the text message is not misleading;
- the text clearly and obviously states that it has been sent for the purpose of direct marketing; and
- the text contains easily understandable instructions for how the individual may opt out of receiving such messages. For the avoidance of doubt, SMS such as "STOP 3764" does not provide enough information to the individual on how they may opt out.

If the direct marketing is via social media, the controller should ensure:

- direct marketing social media communications are sent to the individual only from the controller's official "page" or "profile" on the social media platform; and
- the individual is able to easily respond or get in touch and opt out from such communications from the controller on the same platform.

If the direct marketing is via telephone calls, the controller should ensure:

- the representative begins by identifying themselves and the controller they represent;
- the representative clearly states that the call is a marketing call; and
- if the individual indicates that they would like to opt out or revoke their consent to receive direct marketing that this is recorded and acted upon.

5.3. The requirement to enable individuals to withdraw their consent

Controllers should be able to provide for the right of the individual to withdraw their consent, and if the individual withdraws their consent, they should cease the processing of this individual's personal data for the specific purpose stated. Controllers cannot make it difficult for individuals to withdraw their consent.

Examples:

- An individual has previously consented to receiving direct marketing "newsletters" via email from the controller, each email should include an "unsubscribe" button. Once the individual clicks on "unsubscribe", the controller cannot ask the individual to fill a lengthy form or send an email to the controller providing further personal data. The controller should immediately update their record of consent and provide the individual confirmation that they will no longer receive direct marketing communications unless they "subscribe" to such communications again.
- An individual gets in touch with the controller, withdraws their consent to receiving direct marketing and asks to be excluded from future communications for this purpose. The controller must comply within a reasonable amount of time and may not offer incentives for the individual not to withdraw their consent.

Controllers cannot limit the mechanisms or channels that individuals can use to withdraw their consent for direct marketing and must carry out a request made through any channel, be that via social media or in person at a company premises for example. Controllers must have procedures in place to record when requests are made in such circumstances and carry them out.

5.4. Can controllers rely on third parties to obtain or withdraw consent?

The PDPPL places the obligation on controllers to obtain the individual's consent to receiving direct marketing. Some controllers may use third parties to send direct marketing communications to individuals on their behalf. It is the controller's responsibility to ensure that such third parties:

- Comply with obligations under the PDPPL implementing appropriate administrative, technical and financial precautions and, in particular, obligations under Article 22.
- Have signed a contract with the controller as a joint-controller or processor (for more information on contracts please refer to the Controller and Processor Guidelines).
- Make it clear to individuals that they are acting on behalf of the controller and that the controller is clearly identified as the originator.

Controllers are responsible for direct marketing communications sent on their behalf. If an individual contact a controller to withdraw their consent to, or opt out of, receiving direct marketing communications, they are responsible for ensuring that such communications are not sent on their behalf.

Companies that provide direct marketing services to controllers must ensure that either they or the controller have obtained explicit consent for direct marketing communications to be sent to individuals to. They must also ensure that if such consent is withdrawn, they cease communicating with the individual for the purposes of direct marketing.

Controllers should also ensure that third parties they use to send direct marketing on their behalf do not sell personal data, such as contact details of individuals processed on the controllers behalf, on to other organisations as this would likely not be compatible with the explicit consent provided to the controller.

Controllers must refrain from obtaining "distribution lists" that contain a list of email IDs or mobile numbers of individuals, even if such lists are "anonymised." If individuals on such lists receive direct marketing communications to which they have not consented from or on behalf of a controller, the controller will be held responsible.

6. Further considerations around direct marketing for controllers

In addition to the requirements above, controllers are encouraged to consider the following:

- Incorporating a fit-for-purpose direct marketing governance, policy and procedure framework for the organisation so that the PDPPL requirements are endorsed by senior management and applied across the organisation uniformly.
- Documenting all direct marketing activities in the controller's Record of Processing Activities (RoPA) and keeping the RoPA up to date.
- Ensuring adherence to data privacy by design and conducting a data privacy impact assessment (DPIA) when designing and implementing any direct marketing-related processing activity.
- Ensuring appropriate precautions are taken to reduce the likelihood of a data breach happening which may cause the contact details of individuals to be stolen, altered or destroyed unlawfully.
- Conducting appropriate training on direct marketing for staff involved.

7. What should controllers do about existing direct marketing processes and contact databases?

At the time of introduction of the PDPPL, controllers may already be engaged in sending direct marketing communications to individuals. Such controllers should ensure that they can demonstrate compliance with the PDPPL requirements regarding direct marketing under Article 22 and articulated above. If they are unable to demonstrate compliance with these requirements, controllers are encouraged to:

- Ensure that adequate understandable opt outs are included in all direct marketing communications.
- Review contracts with any third parties the controller is engaged with that carry out direct marketing on their behalf.
- Refrain from sending any new direct marketing communications unless the controller can ensure adherence to requirements.

End of Document