State of Qatar
National Cyber Security Agency

دولة قطر
الوكالة الوطنية للأمن السيبراني

Social Media

PDPPL-02050221E

Guidelines for Individuals

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-02050220E	Individuals' Complaints Guidelines for Individuals (English)
PDPPL-02050214E	Individuals' Complaints Guidelines for Regulated Entities (English)
PDPPL-02050219E	Individuals' Rights Guidelines for Individuals (English)
PDPPL-02050205E	Individuals' Rights 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 organizations 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 "Social Media Guidelines for Individuals".

Any reproduction concerning this document for any purpose will require a written authorization 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 authorization 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 provide individuals with information about how they can protect their personal data and privacy when using social media.
- Individuals should take an active approach to maintaining their privacy when using such platforms.
- Use of social media platforms generates large amounts of personal data. This may not be apparent to individuals. The simple act of "liking" or "sharing" a social media post, for example, may generate information about the individual's location, personal preferences, interests or personality.
- Information shared publicly by individuals on social media is at risk of being obtained and misused by controllers in ways that could cause serious damage to the individuals. Some examples of how personal data posted on social media can be misused by controllers are:
    - Targeted advertising at individuals without consent based on profiling of personal preferences made public.
    - Influencing individuals to take a particular action through social engineering that could put the individual at risk.
    - Using this personal data to influence an individual's political, economic or social understanding following the monitoring of their behaviour.
    - Obtaining or inferring confidential information related to a project due to careless posting by an individual.
    - Creating "fake" accounts impersonating the individual.
- Some examples of steps individuals can take to protect themselves on social media platforms are:
    - Regularly reviewing privacy settings on social media platforms.
    - Limiting the information shared on social media.
    - Maintaining strong passwords for logging into social media platforms.
    - Assessing requests received from other users or accounts to make sure that they are who they say they are and minimising the number of users they connect with to limit the network of individuals and organisations that have access to their social media posts.

2. Introduction

The use of social media platforms often involves sharing personal data. The publicly available and globally-accessible nature of personal data on such platforms means that it is sometimes readily available to individuals, controllers or other actors who may seek to use it to the detriment of the individual(s) that it relates to.

New social media platforms appear regularly, and existing platforms update and add new features almost constantly so individuals should take an active approach to considering their privacy when using such platforms.

These guidelines set out precaution's individuals should take when using social media to protect their personal data and privacy.

3. What is social media and how is it used?

Social media are digital platforms, technologies or services that enable individuals to connect with other individuals, groups or companies to share ideas, information, perhaps trade goods and services and otherwise engage in social networking and virtual communities.

As well as being used by individuals, social media is becoming an increasingly powerful tool that controllers and other actors use by companies to further their interests by engaging with individuals, among other reasons, to:

- improve engagement,
- target marketing,
- increase brand awareness and loyalty, and
- gather feedback to improve their services.

Many controllers target their activities at specific individuals using the personal data that individuals have made public online.

4. How can controllers misuse data shared by individuals on social media?

Using social media poses numerous risks to individuals' privacy and personal data due to the public nature of the platforms and how personal data is stored and shared.

Individuals are constantly exposed to a lot of information that is not necessarily controlled or validated for accuracy or appropriateness and are usually encouraged to share information on social media. Individuals may also be sharing more information than they realise and should be aware that any small activity performed on a social media platform generates data that can be traced back to the individual (hence constituted as personal data). For example, every 'like' or 'share' on a social media platform generates personal data about an individual's interests and this information can be used by organisations to influence the individual to buy a product or service.

Most social media platforms are designed in a way that makes it easy to participate in. Hence, successful social media platforms have increased their number of active users exponentially thereby making more data available to controllers quite easily.

Controllers could have access to the vast amount of data generated by individuals on social media quite easily. Additionally, controllers can obtain personal data on the same individual from multiple social media platforms and combine these datasets.

Such data can be misused for the controller's gain through one of the following:

- Targeted advertising to influence the individual to purchase a product or service. Such targeted advertising is made efficient by appealing to the individual's specific interests, which would not be possible in traditional mass media.
- Stealing an individual's identity by creating a "fake" profile of the individual on the social media platform. This fake profile can be used to obtain confidential information or to influence individuals who will not otherwise be influenced by the "real" profile.
- Social engineering scams that could be used to steal money for individuals, e.g. a malicious entity that sets up a fake online store that steals from individuals by "selling" seemingly real products or services.
- Sale of illicit goods and services which would not be possible via traditional media is made possible on social media. Such sellers target individuals based on the personal data generated by the individual.
- The location of the individual using the social media platform may be visible to controllers.
- Individuals' data can be bundled from more than one social media platform and sold to third parties without the individual's consent or even knowledge.
- Individuals' data may never be deleted from the social media platforms, even if the individual deletes their profile from the social media platform.
- Hackers can use social media to install malicious software on the individual's computers, potentially compromising the individuals personal data.
- Social media platforms may not exercise the appropriate precautions as required by the PDPPL to protect children's data. Children are vulnerable to being easily influenced by such social media platforms.

5. What should individuals do to protect their privacy on social media?

There are a number of steps individuals can take to protect their privacy and personal data when using social media. These include:

- **Review privacy settings**: Individuals should regularly review and update their privacy settings for the social platforms and accounts to reduce the number of people and organisations that can view their activity.
- **Limit sharing of personal information**: Individuals should reduce the personal data they share about themselves online and consider how actors with bad intentions could use such information. Such personal data could be preferences, e.g. 'likes' and 'shares,' images and videos, online quizzes or posts expressing views that could be analysed for key words by computers to identify their views and preferences.
- **Develop understanding of public personal data use:** Individuals should be aware of the extent to which personal data is generated by their actions online and how it could be used to analyse their actions, preferences and beliefs etc. Individuals should also be aware and stay up to date on how such social media platforms can use or misuse the personal data shared or generated on such platforms, especially in light of any reported cases of misuse by the social media platform.
- **Maintain strong passwords**: Individuals should use strong passwords which they should change frequently. Tips for a good password are:
  - Using lengthy passwords, the longer the better.
  - Using numbers, special characters and upper/ lower case letters.
  - Not using obvious personal information (name, city of birth, etc.) that can be guessed by acquaintances.
  - Not using the same password for two or more platforms.
  - Using a trusted password manager application.
  - Changing passwords regularly.
- **Limit "connections" to known individuals**: Individuals should not just accept every connection request they receive online.
- **Do not click suspicious links**: Malicious software, or malware, can easily be distributed online.
- **Report any suspicious activity** on the social media platform itself.
- **Raise a complaint to the National Cyber Governance and Assurance Affairs** about controllers processing personal data in a manner that does not comply with the PDPPL.

For more information on individuals' rights and individuals' complaints please refer to the Individuals' Rights Guidelines and Complaints Guidelines for both Individuals and Regulated Entities.

End of Document