369 DATA SOLUTIONS® PTE. LTD. Data Protection Policy

Effective date : 18 October 2022
Last updated : 18 October 2022

Overview

1. The Personal Data Protection Act (2012) ["PDPA" or "Act"] governs the collection, use and disclosure of personal data by any organisation that does not fall into the definition of a public agency. The Act covers two main sets of obligations for the organisation – **Personal Data Protection** obligations and **Do Not Call** obligations.

2. 369 Data Solutions®Pte. Ltd. takes the above obligations seriously and is committed to put in place reasonable security arrangements to fulfil both sets of obligations. The organisation's data protection policy reflects its attitude toward personal data that has been entrusted with the organisation, so that the individual who provides his or her personal data, does so with an informed context.

Introduction

3. Terms:

3.1	369 Data Solutions®Pte. Ltd.	-"**organisation**";
3.2	Personal Data Protection Policy	- "**pdppolicy**";
3.3	Employee, Customer, User, Individual	- "**data subject**";
3.4	Personal Data Protection Act 2012	- "**PDPA**";

4. The organisation'spdp policy (which may be accessed at: www.369datasol.com) is applicable to the data subject who may interact with the organisation as follows:

   4.1 in the case of customers, users and other stakeholders, through the organisation's:

      4.1.1 offline channel comprising physical location(s) where the organisation conducts its business and business promotion activities;

      4.1.2 online channel comprising the organisation's digital platforms such as the website, mobile application, social media accounts, online store and other digital channels of communication where personal data may be exchanged;

   4.2 in the case of employees, through the relevant departments in the organisation, which will process the personal data in accordance with the specific, employee-related purposes for which the personal data is in the possession or under the control of the organisation.

5. Personal data processing includes the following activities - recording; storing; organising, adapting or altering; retrieving; combination, transmission and erasure or destruction. The organisation recognises that the data subject:

    5.1 provides his or her personal data to the organisation to enable the organisation to conduct its business activities to fulfil the data subject's needs;

    5.2 has rights in relation to the personal data that is in the possession or under the control of the organisation.

Personal data

6. In accordance with Section 2 of the PDPA, and in this Data Protection Policy, personal datarefers to data, whether true or not, about a data subject who can be identified:

    6.1 from that data;

    6.2 from that data and other information to which the organisation has or is likely to have access;

7. The data subject should note that some of the personal data that are in the possession or under the control of the organisation may have been provided to or obtained by the organisation as 'business contact information (BCI)'. BCI refers to an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the data subject, which were not provided by the data subject solely for his or her personal purposes. Certain parts of the PDPA do not apply to such BCI.

8. The personal data that the organisation collects, uses or discloses where necessary:

    8.1 may belong to a minor (children or young persons), defined as those below twenty-one (21) years of age, hence requiring heightened attention from the organisation;

    8.2 may include data types such as: name, audio-visual information related to data subject; NRIC or FIN number; Passport number; Date of Birth; gender; educational qualification; professional qualification; telephone number; residential address; email address; credit card details, device identifier (such as IP address);

    8.3 is kept to a minimum that is necessary for the intended purposes, in line with data minimisation principle.

9. The organisation may collect a data subject's personal data when the data subject or a third-party person interacts with the organisation or the organisation's staff through face-to-face or non face-to-face activities, in relation to any one or combination of the following:

    9.1 making a phone-call conversation with the organisation's customer service staff;

9.2 participating in an interview with the organisation with respect to employment related matters;

9.3 using the organisation's services such as the website, mobile application (app) or social media platforms;

9.4 purchasing the organisation's products or services;

9.5 collecting personal data from a third party person;

9.6 fulfilling commitments for the products purchased;

9.7 signing up for a free trial of the organisation's products or services;

Notification of purpose

10. In accordance with Section 20 of the PDPA, the organisation notifies that the purposes for which the data subject's personal data is collected, used or disclosed are to:

10.1 facilitate the creation, use and maintenance (including update) of accounts belonging to the data subjects (employees or customers or other stakeholders) who interact with the organisation;

10.2 verify the identity of the data subject based on the personal data that is provided;

10.3 facilitate the free trial of the organisation's products and services by the data subject;

10.4 facilitate processing and completion of purchases of the organisation's products and services made by the data subject;

10.5 complete payment processing on behalf of the data subject for his or her purchases;

10.6 provide delivery-of-product services to data subject's delivery address;

10.7 enable the organisation to provide the necessary warranty support for the product purchases made by the data subject;

10.8 to update the data subject on matters related to the product or service that are of interest to the data subject;

10.9 support product warranty arrangements for the data subject;

10.10 enforcement of data subject's repayment obligations;

10.11 support training and quality control by recording the data subject's communications with the organisation;

10.12 manage the organisation's employee with respect to the employee's employment; payment of salary, CPF and other related matters; medical claims and/or payments;

10.13 access to employee work dashboard; and similarly work related requirements;

10.14 business data analytics to improve product and service quality; expand range of products and services;

10.15 promote loyalty programmes; promotional events; lucky draws, contests, competitions and marketing campaigns;

10.16 managing the data subject's ongoing relationship with the organisation;

10.17 analysing the data subject's preferences to ensure that the content, services and advertising that is offered through the organisation's online portals are tailored to the data subject's needs and interests;

10.18 engaging third-party service providers, agents and other organisations to perform any of the functions listed in clause 10.1 to clause 10.18;

10.19 in relation to the use of cookies through our websites and/or mobile applications, the organisation does not use cookies to capture personal data of users of the organisation's website and/or mobileapplications;

10.19.1 essential cookies will be used for the proper functioning of the organisation's digital interfaces with the users;

10.19.2 non-essential cookies may be used for the purpose of powering the organisation's online advertisements as well as managing user interaction with electronic images;

Provision of consent; withdrawal of consent; collection, use and disclosure without consent

11. In accordance with Section 13, 14, 15 and 15A of the PDPA, the organisation will collect, use or disclose the data subject's personal data for the intended purposes through Consent, Deemed Consent or Deemed Consent by Notification from the data subject. The organisation ensures that all consent that is obtained from the individual is valid and is for the intended purposes. Where necessary, the organisation will ensure that the consent is expressly given by the data subject. Any consent given or deemed to have been given to the organisation by a third-party person validly acting on behalf of the data subject is considered valid consent.

12. In accordance with Section 16 of the PDPA, the data subject has the right to withdraw any consent given or deemed to have been given to the organisation, at any time. The

organisation does not prohibit any data subject from withdrawing his or her consent. The organisation is obliged to inform the data subject of the possible consequences for withdrawing consent, including legal consequences, if any, that may arise from the withdrawal of consent. The following steps apply:

12.1 the data subject may submithis or her intention to withdraw consent form by writing to the contact person given in clause 27, who will then follow up formally;

12.2 on receiving the signed 'withdrawal of consent' form from the data subject, the organisation will ensure that the notice is given effect within **21** days of receipt of the signed form; and

12.3 if the withdrawal of notice cannot be given effect within the **21** days, the data subject will be informed in writing, the date within which the said notice can take effect.

13. Provision(s) in the PDPA allow the organisation to collect, use or disclose personal data without consent under certain conditions (for example: under an emergency situation where the life of an individual is threatened). The organisation assures that such conditions are met, before personal data about a data subject is collected, used or disclosed without consent.

Access to and correction of personal data

14. In accordance with Section 21 of the PDPA, the data subject may request access to his or her personal data. The following relate to the request:

14.1 the data subject may submit a request to access his or her personal data by writing to the contact person given in clause 27, who will then follow up formally;

14.2 on receiving the signed 'request to access personal data' form from the data subject, the organisation will, as soon as reasonably possible:

14.2.1 subject to clause 12.3, provide the relevant personal data that is in the organisation's possession or under its control; and

14.2.2 subject to clause 12.3, provide information about the ways in which the personal data may have been used or disclosed within a year before the date of the request;

14.3 the organisation is entitled to levy a reasonable fee on the data subject to fulfil the request. The proposed fee will be given in writing to the data subject. Processing of the request to access personal data will follow upon acceptance of the fee.

15. In accordance with Section 22 of the PDPA, the organisation may receive a request to correct an error or omission in the personal data of a data subject; that is in the organisation's possession or control. The following steps relate to the request:

15.1 the data subject may submit a request form, to correct an error or omission in his or her personal data by writing to the contact person given in clause 27, who will then follow up formally;

15.2 if the organisation is satisfied that there are no reasonable grounds to deny the request, the organisation will:

15.2.1 subject to clause 16, correct the personal data as soon as practicable; and

15.2.2 send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date of correction was made unless:

15.2.2.1 the other organisation does not need the corrected personal data for any legal or business purpose;

15.2.2.2 with the data subject's consent, send the corrected personal data only to specific organisations to which the personal data was disclosed by the organisation within a year before the date of correction was made;

15.3 If the organisation is notified of a correction of personal data by a third-party person, the organisation will correct the personal data that is in the organisation's possession or under its control.

16. With respect to clause 14 and clause 15 – request to access personal data and request to correct personal data respectively – the following apply:

16.1 should the organisation not be able to respond to the request within thirty (30) calendar days after receiving the request, the data subject will be informed in writing within the thirty (30) calendar days of the date by which the organisation will be able to respond to the request;

16.2 provision(s) in the PDPA allow the organisation, under certain conditions, to deny the data subject's request to access or correct the personal data. Generally, the organisation will inform the data subject of the reasons for denying the request (except where the organisation is not required to do so under the PDPA).

Accuracy of personal data

17. In accordance with Section 23 of the PDPA, the organisation makes reasonable effort to ensure that the personal data collected by or on behalf of the organisation is current, complete and accurate if the personal data is likely to be:

17.1 used by the organisation to make a decision that affects the data subject to whom the personal data relates to; or

17.2 disclosed by the organisation to a third party.

Accordingly, the data subject may be approached by the organisation periodically to assist in updating his or her personal data, or the data subject should update the organisation through the contact details in clause 27 if there are changes to his or her personal data.

Protection of personal data

18. In accordance with Section 24 of the PDPA, the organisationendeavours to put in place reasonable security arrangements to protect the data subject's personal data, which includes personal data stored in electronic and non-electronic formats, to facilitate data processing safely. Accordingly, the organisation has implemented reasonable administrative, physical and technical measures (such as up-to-date anti-virus protection, encryption, use of privacy filters to secure storage and transmission of personal data, applying the principle of need-to-know when accessing or disclosing personal data both internally and externally to relevant stakeholders, physical security of storage premises, training of employees) are in place to protect the personal data that is in the organisation's possession or control, to prevent:

    18.1 unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and

    18.2 the loss of any storage medium or device on which personal data may be stored.

19. The data subject should take note that no method of transmission over the internet or method of electronic storage, or otherwise, is completely secure. While security cannot be guaranteed, the organisation strives to protect the security of the personal data and constantly reviews and enhances its personal data protection measures.

Retention of personal data

20. In accordance with Section 25 of the PDPA, the organisation will stop retaining personal data, or remove the means by which the personal data can be associated with the data subject, as soon as it is determined that:

    20.1 the purpose for which the personal data was collected is no longer being served by retaining the personal data; and

    20.2 retention of the personal data is no longer necessary for legal or business purposes.

21. The personal data may either be anonymized or disposed depending on the circumstances. Anonymisation refers to rendering the personal data not being able to be used to identify the data subject any longer. Disposal of the personal data refers to the deletion, erasure or destruction of the personal data, and where necessary, may include the destruction of the media on which the personal data is stored.

Transfer or personal data outside Singapore

22. The organisation leverages the cloud-based services provided by Amazon Web Services (AWS) and uses AWS's Singapore based server. Generally, all the personal data collected by the organisation will be processed in Singapore. All stakeholders whose personal data is collected by the organisation may note that his or her personal data is retained within the Singapore-based server of AWS. The organisation assures that retention of such personal data will be in accordance with clauses 20 and 21.

23. The organisation recognises that personal data that is in its possession or under its control may be required to be transferred outside Singapore for the performance of the organisation's contractual obligations with the data subject. In accordance with Section 26 of the PDPA, the organisation is obliged to ensure that for the personal data transferred out of Singapore, it provides a standard of protection that is comparable to the protection under the PDPA. To that end, the organisation assures that the choice of data processing and cloud service provider(s) in the recipient jurisdiction is considered thoroughly to take into account the requirements related to transfer of personal data outside Singapore.

Do Not Call obligations

24. The organisation conducts its marketing and promotional activities of its products and services in accordance with the Do Not Call provisions of Part 9 of the PDPA. If the organisation has obtained a Singapore telephone number(s) belonging to a data subject who has expressly given consent to the receipt of marketing and promotional content, the organisation may use such telephone numbers to engage the data subject with respect to its product and service offerings.

25. In relation to conducting marketing and promotional activities via Singapore telephone number(s), the organisation will exercise its duty to check and verify that the Singapore telephone number can be called for the purpose of conducting its marketing and promotional activities.

Data breach management

26. Despite the best efforts by the organisation to protect the personal data that is in its possession or under its control, a personal data breach incident may possibly occur. The organisation assures that a personal data breach incident management mechanism is in place, in accordance with Section 26A to 26D of the PDPA, to deal with a personal data breach incident. Some of the key aspects of the mechanism relates to:

    26.1 investigating the personal data breach in a reasonable and expeditious manner;

    26.2 ensuring the organisation's data intermediary has a mechanism in place to notify the organisation expeditiously, of any occurrence of a personal data breach;

26.3 determining whether the personal data breach is a notifiable data breach;

26.4 notifying the relevant persons;

26.5 activating a communications plan.

Data Protection Officer contact details

27. The organisation updates its pdp policy periodically to ensure that the pdp policy is consistent with the prevailing data protection legislation(s), business practices and technology trends. Any queries with respect to the organisation's pdp policy may be directed to:

27.1 Email: dpo@369datasol.com