LYK MOBILE PTE. LTD.
ORGANISATION DATA PROTECTION POLICY

Contents

Organisation Data Protection Policy

Our organisation (LYK Mobile) has put together this Data Protection (DP) Policy to help you with data protection policies, practices and complaint-handling process to comply with the Personal Data Protection Act within our organisation. This policy contains useful information and resources such as forms, clauses and communication material. It will also guide you through common issues that you may face in complying with Data Protection (DP) and Do Not Call (DNC) provisions.

About The PDPA

The Personal Data Protection Act (PDPA) governs the collection, use and disclosure of personal data by organisations, in a manner that recognises individuals' rights and the need of organisations to use such personal data for legitimate business purposes. The personal data includes full name, passport number, National Registration Identity Card (NRIC) number or Foreign Identification Number (FIN), thumbprint, personal mobile telephone number, iris image, DNA profile, voice recording of an individual, and photograph or video image of an individual.

The PDPA contains two main sets of provisions; namely Data Protection (DP) provisions and the Do Not Call (DNC) provisions.

9 Data Protection Obligations

<u>Collection, use and disclosure of personal data</u>

Consent
- Obtain consent to collect, use or disclose individuals' personal data.
- Allow individuals to withdraw consent.

Purpose
- Do not make customers consent to the collection, use or disclosure of their personal data beyond what is reasonable to provide the product or service.
- Collect, use or disclose personal data only for the purposes for which consent was obtained.

Notification
- Notify individuals of the purposes for the collection, use or disclosure of their personal data.

<u>Accountability to individuals</u>

Access and Correction
- Upon request, provide individuals with their personal data and the ways in which their personal data were collected, used or disclosed in the past year.

• Correct any error or omission in individuals' personal data upon their request.

Openness
• Make Data Protection Officer's business contact information readily available to the public.

Care of personal data

Protection
• Put in place reasonable security arrangements to protect personal data from unauthorised access, collection, use, disclosure and similar risks.
• Make reasonable effort to ensure that the personal data collected is accurate and complete.

Accuracy
• Make reasonable effort to ensure that the personal data collected is accurate and complete.

Retention
• Cease retention or anonymise personal data when it is no longer necessary for any business or legal purposes.

Transfers
• Ensure that the standard of protection accorded to personal data is comparable to the PDPA when it is transferred overseas.

Data intermediaries that process personal data for our organisation under contract must meet the protection and retention requirements under the PDPA.

Do Not Call (DNC) Provisions

Do not send certain marketing messages to Singapore telephone numbers including mobile, fixed line, residential and business numbers registered with the DNC Registry.

Check The DNC Registry

Before sending a marketing message to a Singapore telephone number, you must check the DNC Registry established by the PDPC to confirm that the Singapore telephone numbers on your marketing list are not registered, unless you have obtained clear and unambiguous consent to send the marketing message to the user or subscriber of that number.

Data Protection Officer

Our organisation has appointed one person who is part of the management team as the Data Protection Officer (DPO).

Our DPO is Ms Sophia Yap. You can forward all PDPA-related queries and complaints to her.

What DPO Does

• Ensures compliance of PDPA when developing and implementing policies and processes for handling personal data;
• Fosters a data protection culture among employees and communicate personal data protection policies to stakeholders;
• Manages personal data protection-related queries and complaints;
• Alerts management to any risks that might arise with regard to personal data; and
• Liaises with the PDPC on data protection matters, if necessary.

DPO Business Contact Information

Our DPO can be easily contacted by the public. She is registered with PDPC at www.pdpc.gov.sg/dpo-contact.

The appointment of a DPO is a mandatory requirement under the PDPA. The DPO is an important driver to ensure our organisation's data protection measures are adequate.

Notify Purpose(s) And Seek Consent

Below are some steps to follow when collecting personal data:

1 Consider whether it is reasonable to request the personal data to provide the product or service

2 Notify the customer of our purpose for collecting, using or disclosing his/her personal data

3 Seek his/her consent

4 Allow him/her to withdraw consent
at any time
Personal data should only be collected for reasonable purposes which have been notified to the individual in advance and for which the individual has consented, unless collection without consent is permitted or required under the PDPA or any other written law.

Conducting Lucky Draws

It is important to inform the individual that we are collecting, using or disclosing his personal data for a lucky draw and to obtain consent for that purpose. If you plan to use the personal data for some other purpose outside of the administration of the lucky draw, you must state so clearly.

Withdrawal Of Consent

An individual may at any time withdraw consent that he/she had given to our organisation for the collection, use or disclosure of his/her personal data.

When you receive a request to withdraw consent,

• You must inform the individual of the likely consequences of withdrawing his/her consent. You must stop using his/her personal data after the withdrawal. Do not keep the personal data if you have no business or legal purpose to do so.

• If it requires more than 10 business days to effect the withdrawal notice, inform the individual when he/she can expect the withdrawal of consent to take effect.

• Similarly, if an individual opts out of receiving our organisation's telemarketing messages, you must ensure that such messages will no longer be sent to his/her Singapore telephone number by the end of 30 days.

Opting Out Of Receiving Telemarketing Text Messages

In your telemarketing messages, you may provide information on how individuals can opt out of such messages. Indicate clearly what types of marketing message the withdrawal will affect. If the withdrawal notice is unclear, it may be considered an optout of all marketing materials sent via that medium.

Notify When Taking Photographs Or Videos

You should inform individuals when you are taking photographs or videos of them at an event that our organisation hosts, or if you have closed-circuit televisions (CCTVs) monitoring our organisation's premises and recording images of visitors.

Your notice should state the purpose of the CCTVs (for example, for security purposes). You must clearly print and place notices in areas that are easily visible. You do not need to indicate the exact location of our CCTV cameras.

When taking photographs or recording videos at events, notify attendees by using signages at the event and/or even before they sign up for it, such as via the registration form.

You can also state the purposes on the invitation card or the registration form for the event. If you intend to rely on notices at the function venue, you should ensure that the notices are easily visible to all attendees, e.g., by placing obvious notices at the reception and entrances to the venue.

Respond When Individuals Ask About Their Personal Data

When our customer wants to know what personal data we have collected about him/her and how it has been used and disclosed in the past year, you must provide that information as soon as reasonably possible. You may charge a reasonable fee to cover the processing cost for the request, provided that you give a written estimate of the fee beforehand.

If you are unable to provide it within 30 days, you must inform the individual within 30 days and let him/her know when you can respond.

Individuals may submit an access request in person, through email or by post.

Keep a record of all access requests, and indicate whether the request was granted or rejected. This will help you in the event of a dispute. As part of our organisation's documentation process, use an acknowledgement form.

Allow Correction Of Personal Data

When an individual requests to correct an error or omission in his personal data, you must do so, unless an exception applies.

Secure The Personal Data Held By Our Organisation

There are established security arrangements to protect the personal data under our organisation. This is to prevent unauthorised access, collection, use or disclosure of the data and other similar risks.

Protect Our Electronic Data

AT EMPLOYEE LEVEL

• Encrypt or password protect any personal data held electronically that would cause harm if lost or stolen, such as in portable computing devices and documents. This includes email attachments containing personal data. If sending to another party, communicate the password separately.

• Regularly back up information on computer systems and keep the backups in a separate location.

• Dispose properly documents containing personal data that are no longer needed. Use specialised software tools to erase personal data stored on hard disks or degauss hard disks.

AT ORGANISATION LEVEL

• Install firewalls and virus-checking software on employees' computers.

• Limit employee access to sensitive and confidential documents on a need-to-know basis.

• Secure portable computing devices when not in use by locking them up or attaching them to a fixture by a security cable.

• Use privacy filters, careful positioning of your computers and other means to prevent unauthorised persons from viewing your computer screens.

• Set computer screens to lock automatically when left unattended for a specified period.

• Secure websites and applications (apps). Files containing personal data should not be made available online.

• Restrict use of external devices on all company-issued computers to authorised persons only.

• Check that our appointed software developers keep pace with ICT security threats, and are able to design and maintain ICT systems with the capacity to protect stored personal data.

Personal Data Breach

Data breaches can happen despite all the precautions that we may take, for various reasons. If it does, start by capturing full information about the data breach before proceeding with an investigation.

Dispose Of Personal Data That Is No Longer Needed

Stop holding on to personal data when you no longer have any business or legal use for it.

This means that you should:

1. Set a retention period for various types of personal data

Categorise the personal data and decide how long it should be retained. Keep personal data only as long as there is a business or legal purpose.

2. Safely dispose of personal data when you no longer need them

1 For paper such as documents and photos

Shred, pulp or incinerate them.

2 For electronic media

USB sticks and hard disks/SSDs:
Use specialised software to overwrite selected files or entire medium.

Write-once or read-only CDs, DVDs and other media that do not support overwriting:
Crush, drill, shred or otherwise physically destroy the medium.

Ensure Protection Of Personal Data When Transferring Overseas

If you intend to transfer personal data overseas, do take steps to ensure that the data protected in compliance with the PDPA while the personal data is still in our possession or control.

Should the transfer be to another organisation overseas, you must also ensure that the receiving organisation is bound by legally enforceable obligations to provide protection comparable to the standard under the PDPA. Such legally enforceable obligations may be imposed by law or by entering into a contract with the recipient.

Alternatively, personal data may be transferred overseas to another organisation if it falls within other prescribed circumstances, such as if:

• the individual has been informed of the level of protection that will be accorded to his/her personal data as compared to the PDPA and consents to the transfer of the personal data to that recipient in that country or territory;

• the transfer is necessary for the performance of a contract between our organisation and the individual; or

• the personal data is publicly available in Singapore.

Closely Manage Service Providers That Handle Personal Data

If we engage a service provider to process personal data (this includes hosting, storing or processing the data), we may be held responsible if our service provider contravenes the PDPA while providing the service to us.

When entering into a service agreement with a service provider, ensure there are clauses that require them to take sufficient measures to ensure compliance with PDPA requirements.

Contracts alone are not the end of our accountability. You should also establish relevant standard operating procedures (SOPs) for our service provider on the processing of personal data, and include measures to monitor its compliance with these SOPs.

Check The Do Not Call Registry

If you conduct telemarketing to subscribers or users of Singapore telephone numbers, you will need to submit the telephone numbers on your telemarketing list for checks against the Do Not Call (DNC) Registry, unless the subscriber or user has given his/her clear and unambiguous consent to receive such messages.

To check the DNC Registry:

Create an Account

Our organisation has a main account on the DNC Registry website. Each main account gets 1,000 free credits every year, valid for one year from date of issue.

Check the Registry

Check telephone numbers against all 3 DNC registers for voice calls, texts and faxes. There will be a charge for each number submitted for checking, regardless of whether the number has been submitted before.

Receive the results

You receive results for Small Number Lookup of telephone numbers (10 or less numbers at one time) immediately. For a bigger list, use Bulk Filtering. You will receive the results in less than 24 hours. All results are valid up to 30 days. Thereafter, you will need to re-check the DNC Registry.

Communicate Our Data Protection Policies, Practices And Processes

For our Customers:

• Provide the business contact information of our DPO so that our customers can contact him/her for PDPA-related queries or complaints.

• Readily provide information about our data protection policies, practices and complaint process upon request.

For our Employees:

Communication

• Inform all employees of our data protection policies and practices. Make sure they know and adhere to our processes for protecting personal data. Emphasise their roles in safeguarding personal data and ensuring that our organisation complies with the PDPA.

• Use posters, email and other communication tools to raise awareness of the importance of personal data protection among our staff.

Appendices

i) Consent Clause for Membership Application

ii) Consent Clause for Sending Marketing Materials

iii) Consent Clause for Lucky Draws

iv) Consent Clause for Job Applicants

v) Acknowledgement and Consent Clause for Supplying and Marketing Business-to-Consumer Goods and/or Services

vi) Clause for Individuals to Withdraw Consent Given for Receiving Marketing Materials

vii) Clause to Let Individuals Opt Out of Receiving Telemarketing Messages

viii) Notice to Inform Individuals of CCTV Recordings on Our Premises

ix) Notice to Inform Individuals of Photography or Video Recording at Events

x) Forms for Access Request and Acknowledgement

xi) Form for Correction Request

xii) Personal Data Breach Report