KULICKE & SOFFA PTE. LTD.

GLOBAL DATA PROTECTION POLICY – SINGAPORE ADDENDUM/POLICY

GLOBAL DATA PROTECTION POLICY - SINGAPORE ADDENDUM/POLICY
KULICKE & SOFFA PTE. LTD.

1. INTRODUCTION

1.1 Background To The Personal Data Protection Act 2012

1.1.1 The Personal Data Protection Act 2012 (the "**PDPA**") is intended to be a baseline law for the protection of personal data in Singapore. The Personal Data Protection Commission ("**PDPC**") was established on 2 January 2013 to administer and enforce the PDPA. The PDPA is applicable to Kulicke & Soffa Pte. Ltd. (referred to as the "**Organization**") and the Organization is committed to complying with it.

1.2 Background to Singapore Addendum/Policy

1.2.1 This Singapore Addendum/Policy (the "**Singapore Policy**") supplements the global data protection policy (the "**Global Data Protection Policy**") of Kulicke and Soffa Industries, Inc. and/or any of its affiliates (collectively, "**K&S**") and should be read together as one policy. Save as set out in this Singapore Policy, all other terms and principles in the Global Data Protection Policy shall continue to apply. The Singapore Policy shall apply to all K&S entities incorporated in Singapore and all processing of personal data by K&S in Singapore.

1.2.2 This Singapore Policy shall prevail in the event of inconsistency between the principles or contents stated herein and those as described under the Global Data Protection Policy.

1.2.3 In this Singapore Policy, you will see the word "**process**" or "**processing**" being used in relation to personal data. Essentially, it means carrying out any activity in relation to personal data including collecting, using, disclosing, holding, transmitting, destroying etc.

1.3 Singapore Addendum/Policy Part Of Employment Contract

1.3.1 All employees and agents of the Organization must strictly comply with this Singapore Policy. For employees of the Organization, this Singapore Policy binds each employee and forms a part of the terms of the employment contract between the Organization and the employee.

1.3.2 The Organization reserves its right to amend this Singapore Policy from time to time. Any such amended Singapore Policy will similarly apply to you and become part of your employment contract with the Organization from the time of such amendment taking effect.

1.3.3 This Singapore Policy seeks to provide each employee with a broad summary overview of the requirements of the PDPA and an understanding of the PDPA's impact on operational activities. For detailed information on the obligations and exceptions under the PDPA, you may refer to the PDPA itself as well as guidelines from the PDPC at **www.pdpc.gov.sg**.

1.4 The Organization's Data Protection Officer

1.4.1 The Organization will have one or more Data Protection Officers. If in doubt on any aspect of the PDPA or this Singapore Policy, please do not hesitate to contact the Data Protection Officer. You must comply with any directions and instructions of the Organization's Data Protection Officer(s).

1.4.2 The details of the Data Protection Officers can be found in the Global Data Protection Policy under the section heading "Data Protection Committee".

1.5 What To Do If You Are Aware Of Or Suspect A PDPA Breach

1.5.1 If you have information or become aware that a breach under the Singapore Policy, Global Data Protection Policy or otherwise under the PDPA has occurred within the Organization, please report it immediately to the Data Protection Officer.

2. OVERVIEW OF THE PERSONAL DATA PROTECTION ACT 2012

2.1 The PDPA Obligations Applicable To Personal Data

2.1.1 With regard to dealing with personal data of any individuals, the Organization and all employees are required to adhere to the following key **data protection principles/obligations** :

(a) Consent;

(b) Purpose Limitation;

(c) Notification;

(d) Access and Correction;

(e) Accuracy;

(f) Protection;

(g) Retention Limitation;

(h) Transfer Limitation;

(i) Accountability; and

(j) Data Breach Notification.

(the above data protection principles/obligations may be referred to in this document as the "**data protection principles**")

3. THE CONSENT OBLIGATION / PRINCIPLE

3.1 Introduction

3.1.1 Under the PDPA, the Organization must obtain the consent of the individual for the collection, use or disclosure of his personal data for any purpose, and such consent must be obtained prior to such collection, use or disclosure, unless an exception to the requirement of consent applies.

3.2 Express And Deemed Consent

3.2.1 Consent may be express or deemed. Deemed consent can take three forms: (a) deemed consent by conduct; (b) deemed consent by contractual necessity; and (c) deemed consent by notification.

3.2.2 As far as possible, express consent should be obtained. Check with the Data Protection Officer or the Organization's management if you are seeking to obtain consent other than by express means. The Data Protection Officer can make a determination of whether your factual circumstance allows for the application of one of the forms of deemed consent.

3.2.3 You are to obtain consent in writing by using the issued form(s) and wording(s) approved and provided by the Organization's management. Do not use form(s) or wording which have not been approved by the Data Protection Officer or the Organization's management.

3.2.4 In dealing with the consent principle and the purpose principle (elaborated below), the Organization has undertaken various compliance measures. This includes but is not limited to (where relevant) :

(a) ensuring that individuals are notified of purposes for which their personal data may be processed by the Organization and their respective consents obtained (in some cases such as CCTV signages (where relevant), the Organization will rely on the deemed consent concept);

(b) amending forms/documents where necessary;

(c) amending terms and conditions governing the customer relationship and/or the Organization's relationship with data intermediaries and other business partners, to deal with the PDPA;

(d) amending the human resource related documents such as employment contract terms; and/or

(e) CCTV signage notification.

3.2.5 Do ensure that you now deploy and use materials and processes, such as those above, which have been created or modified, to deal with the PDPA.

3.3 Consent As A Result Of False Or Misleading Information

Take note that consent will be invalid where it is given as a result of false or misleading information or has been obtained through deceptive or misleading practices. Thus all employees will need to ensure that they do not misrepresent, mislead or provide false information whenever consent is being obtained from individuals.

3.4 Obtaining Personal Data From Third Parties

In many situations, the Organization will/may be collecting personal data from third parties other than the individual himself (these third parties could be corporations or individuals). In these situations, no such collection should be engaged in unless the employee is satisfied that the third party providing the personal data of individuals has obtained the consent of those individuals to disclose their personal data to the Organization for the specified purpose(s) and that those individuals have indeed consented to the Organization collecting, using and disclosing their personal data for the specified purpose(s). Please consult the Data Protection Officer if you have questions relating to this Section 3.4.

3.5 Disclosing Personal Data to Third Parties and Data Intermediaries

3.5.1 Where the Organization intends to disclose personal data to third parties (such third parties may or may not be data intermediaries) for certain purposes, it must obtain the consent of the individual for the disclosure of his personal data by the Organization to the third party for such purpose(s). These purpose(s) must have been notified to the individual and that individual's consent obtained prior to disclosure to the third party, unless an exception to the requirement of consent under the PDPA applies. A data intermediary is essentially an organization that processes personal data on behalf of the Organization. A data intermediary could be a recruitment agency, a third party data hosting provider, a courier service provider, a security company, a marketing company, a service provider which sends out marketing messages on the Organization's behalf, etc..

3.5.2 Prior to the disclosure, transfer or sharing of personal data, ensure that the personal data you are going to provide is only that which is necessary for the receiving party(ies)' purposes and that the personal data disclosed is consistent with the consent given by the individual (unless an exception to the requirement of consent under the PDPA applies). You should also take note of or maintain a record of, personal data that has been provided to and received from third parties. This is to enable the Organization to deal with the access and correction principles.

3.5.3 Prior to disclosing personal data to the third party recipient, ensure that standard contractual provisions have been imposed on the third party recipient to protect such personal data. When in doubt on whether this has been achieved or on the wording of the contractual provisions, contact the Organization's Data Protection Officer.

3.5.4 An organization has the same obligations in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organization itself. This effectively means that, in using a data intermediary, the Organization remains primarily responsible for the actions and omissions of its data intermediary when the data intermediary is processing personal data for the Organization.

3.5.5 In this regard, to protect itself, the Organization will have to contractually impose obligations on its data intermediaries to process personal data in accordance with the PDPA so as to ensure the Organization's compliance with and to limit its liability under the PDPA. You must seek approval from the Organization's management or Data Protection Officer before engaging any data intermediary. You must also ensure that a written contract with suitable clauses is in place. You may obtain such clauses from the Organization's management or Data Protection Officer.

3.6 Where the Organization is processing personal data on behalf of another organization, be sure that there is a written contract in place with this organization prior to the engagement in any activity on their behalf. Do not proceed with such activity unless the Organization's management or Data Protection Officer has approved it.

3.7 Disclosing Personal Data To Public Agencies

3.7.1 When you receive a request from a public agency for disclosure of personal data, immediately notify the Organization's management or Data Protection Officer and await further instructions. Do not disclose any personal data until the Organization's management or Data Protection Officer has given approval to do so. The Organization's management or Data Protection Officer may also instruct you to obtain further information from the public agency prior to disclosing the personal data.

3.8 Exceptions To The Requirement of Consent

3.8.1 The Organization may collect, use or disclose personal data without the individual's consent in limited circumstances. Approach the Data Protection Officer for more information on exceptions that may apply to you. Do note that relying on an exception does not exempt the Organization from having to comply with the remaining data protection principles as such an exception is only an exception to the consent and purpose principles.

3.9 Dealing With Corporate Clients

3.9.1 Customers would usually be corporations. In the case of corporations, in dealing with such corporate customers, the Organization would foreseeably be collecting and processing personal data of staff of its corporate customers, including directors, shareholders, designated employees of the corporate customer. The Organization need not abide by the data protection principles when dealing with personal data where the personal data constitutes Business Contact Information ("**BCI**").

3.9.2 The PDPA defines BCI as:

"*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 individual, not provided by the individual solely for his personal purposes.*"

3.9.3 When personal data falls under the BCI definition, such personal data is not subject to the key data protection principles, i.e. the key data protection principles referred to at paragraph **2.1.1** above do not apply to BCI.

3.9.4 Please note that the provisions relating to the DNC regime (explained below) will still apply to BCI. This is because the DNC regime is separate from the data protection principles. In this regard, the DNC requirements (explained below) would be applicable and would need to be complied with.

3.9.5 If you are not sure about whether personal data falls within the scope of BCI, please contact the Data Protection Officer.

3.10 Withdrawal Of Consent

3.10.1 An individual is entitled to withdraw his consent for the Organization to process his personal data at any time. An individual who has previously consented to the collection, use or disclosure of his personal data for notified purposes can withdraw his consent at any time upon giving reasonable notice.

3.10.2 The Organization or you, cannot prohibit an individual from withdrawing his consent. Upon receipt of a notice of withdrawal from an individual, which can come in any form such as an email, a letter, verbal notification etc. to any employee or representative of the Organization, the Organization must immediately deal with such withdrawal of consent.

3.10.3 You must not ignore any communication from an individual wherein the individual seeks to withdraw his consent. Immediately notify the Data Protection Officer and the Organization's management should you receive a request for withdrawal of consent.

3.11 Consent For Marketing

3.11.1 When you intend to collect, use or disclose an individual's personal data for marketing purpose, such as to send that individual marketing brochures, you must notify that individual about the Organization's intended processing of his personal data for marketing purpose and obtain that individual's consent. When seeking to obtain consent for marketing purpose, please ensure that you only use form(s) which have been approved by the Organization's management or Data Protection Officer.

3.11.2 Any consent that is sought to be obtained from an individual, for the Organization to send that individual marketing information or materials, must be by way of an opt-in consent. This is regardless of the mode of communication of the intended marketing information. This means that traditional modes of communication such as email or postal mail, can only be done if the Organization has obtained opt-in consent. Opt-out consent is not permitted. Before embarking on the sending of any marketing information, check with your Data Protection Officer that the opt-in consent of the intended individual recipient had been obtained. If you intend to send marketing information or materials by way of the Do Not Call regime modes of communication, namely voice call, text messages or fax, consult the Data Protection Officer on what you need to do, before you can do so.

3.11.3 Where you intend to send a marketing message to a Singapore telephone number, be sure that (a) you have obtained the necessary consent from the individual for the collection, use or disclosure of his personal data for marketing purposes; and (b) you adhere to the requirements of the DNC regime (defined and explained below).

4. PURPOSE LIMITATION AND NOTIFICATION OF PURPOSE OBLIGATIONS – PURPOSE PRINCIPLE

4.1 Introduction

4.1.1 The Organization may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances, which have been notified to the individual concerned. Please note that when providing notification of purposes, these should be provided to the individual before or at the very latest, at the time of collecting the individual's personal data.

4.1.2 For any purpose that is new or intended for future collection, use or disclosure, fresh consent needs to be obtained from the individual in question before you can process that individual's personal data for such new purpose.

4.2 Notification That Photographs / Videos Will Be Taken At Events

4.2.1 The taking of photograph(s) of an individual or the taking of a video of an individual constitutes the collection of personal data. Accordingly, the consent and purpose principles must be complied with. Note also that once such photograph or video is taken, the Organization would also need to deal with the other data protection principles with regard to such photograph or video, such as access rights, protection principle etc.

4.2.2 Where such photograph or video is to be taken in a closed door event and in a place that is not open to the public, the consent of the individual whose image is to be taken has to be obtained, preferably in written form. There may be also a need to have other provisions in the written consent to deal with use of that individual's image rights. In such a case, seek the approval of the Organization's management or Data Protection Officer on the wording of the consent form before deploying the written consent.

4.3 Log Books And Other Record Books

4.3.1 Where log books are used, for example at security counters or at the reception, a process / procedure should be implemented to ensure that there is no inadvertent disclosure of an individual's personal data during the use of such books.

4.4 CCTV And Other Surveillance

4.4.1 Where CCTV cameras are being used to record visitors to the compound, notices should be placed prominently at all major entrances. Such notices will serve to notify individuals that their personal data may be collected via the CCTV systems in place.

4.4.2 Where a third party service provider has been engaged to provide or operate the CCTV system, the contract with such third party should have clauses inserted dealing with the PDPA. Please consult the Data Protection Officer for the appropriate data intermediary clauses.

5. ACCESS OBLIGATION / PRINCIPLE

5.1 Introduction

5.1.1 Pursuant to the access principle under the PDPA, any individual has the right to request from an organization the following:

(a) details of personal data of the individual that is in the Organization's possession or under the Organization's control; and

(b) information on how the Organization has used or disclosed, or may have used or disclosed such personal data, in the one (1) year preceding the date of the individual's request.

5.1.2 The Organization must respond to each access request as accurately and completely as necessary and reasonably possible.

5.1.3 When you receive a request (whether in writing or otherwise), you must immediately notify the Data Protection Officer and the Organization's management. There is a short period of time by which the Organization must respond to the requestor. There are circumstances when the Organization and you must not provide an individual information about his personal data

and how it has been used or disclosed, in response to his access request. This will be dealt with by the Data Protection Officer or the Organization's management**.**

6. CORRECTION OBLIGATION / PRINCIPLE

6.1 Introduction

6.1.1 Under the PDPA, any individual may request the Organization to correct an error or omission in the individual's personal data that is in the Organization's possession or under its control. Upon receipt of a correction request from an individual, the Organization shall:

(a) correct the personal data as soon as practicable; and

(b) send the corrected personal data to every other organization(s) to which the personal data was disclosed by the Organization within a year before the date the correction was made, unless:

(i) those other organization(s) do/does not need the corrected personal data for any legal or business purpose; or

(ii) the Organization has the consent of the individual to only send the corrected personal data to specific organizations to which the personal data was disclosed within a year before the date the correction was made.

6.2 Notification Of Correction Requests By Other Organizations

6.2.1 The Organization may also in turn, receive correction requests from other organizations who have disclosed personal data to it. Where such a request has been received, the Organization should correct the personal data in its possession or control accordingly, unless the Organization is satisfied on reasonable grounds that the correction should not be made.

6.3 Dealing With Correction Requests

6.3.1 When acting on correction requests received by the Organization, the Organization would as a default have to correct the individual's personal data pursuant to the correction request.

6.3.2 When you receive a request (whether in writing or otherwise), you must act on such requests by immediately notifying the Data Protection Officer and the Organization's management. There is a short period of time by which the Organization must respond to the requestor. The Organization is entitled to refuse to correct an individual's personal data in response to a correction request received from that individual in certain situations. This will be dealt with by the Data Protection Officer or the Organization's management.

7. ACCURACY OBLIGATION / PRINCIPLE

7.1 Introduction

7.1.1 Pursuant to the accuracy principle under the PDPA, the Organization must make a reasonable effort to ensure that personal data collected by it or on its behalf is accurate and complete if the personal data :

(a) is likely to be used by the Organization to make a decision that affects the individual concerned; or

(b) is likely to be disclosed by the Organization to another organization.

7.2 Compliance with the Obligation

7.2.1 In order to comply with the accuracy principle, the Organization and you must ensure that :

(a) all personal data of individuals that is collected (whether directly or from a third party) is accurate and correctly recorded. Without limiting what you need to do in order to deal with this, one method could be to verify personal data provided by an individual with original source documents provided by that individual;

(b) the personal data of individuals collected includes all relevant parts thereof;

(c) all appropriate steps have been taken in the circumstances to ensure the accuracy and correctness of the personal data; and

(d) consideration be given as to whether it is necessary to update the personal data that had been collected and if so, to put in place measures to do so.

7.2.2 If you rely on third party data intermediaries or service providers to provide you with personal data of individuals, you must ensure that the personal data of individuals that they provide to the Organization is accurate and complete.

8. PROTECTION OBLIGATION / PRINCIPLE

8.1 Introduction

8.1.1 Pursuant to the protection principle under the PDPA, the Organization must protect personal data in its possession or under its control (whether in physical or electronic form) by making reasonable security arrangements to prevent :

(a) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks; and

(b) the loss of any storage medium or device on which personal data is stored.

8.1.2 There are various aspects to the Organization's compliance with its personal data security obligations. Security arrangements should include measures such as a combination of administrative measures, physical measures and technical measures. The Organization's management will be considering and implementing what protective measures are needed appropriate to the personal data in question.

9. RETENTION LIMITATION OBLIGATION / PRINCIPLE

9.1 Introduction

9.1.1 Pursuant to the retention principle in the PDPA, the Organization must cease to retain documents containing personal data (i.e. to destroy documents containing personal data or to delete/destroy personal data) or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that :

(a) the personal data no longer serves or is no longer needed for, the purpose(s) for which it was collected; and

(b) such personal data is no longer required for business or legal purposes.

9.2 Ceasing To Retain

9.2.1 With regard to the obligation to destroy personal data, in carrying out such destruction, it should cover not only personal data in the Organization's IT systems and hardcopy personal data, but those of its data intermediaries, in back-ups, as well as softcopies in employees' computers and those physical copies kept in files or physically kept by storage vendors. In

other words, as an example, simply deleting an individual's personal data from a staff's desktop computer is insufficient – one needs to delete other copies kept in other repositories such as hard copies, backups, etc.

9.2.2 Where you or your department is the point of contact with a data intermediary, you must ensure that the data intermediary securely destroys all personal data after the data intermediary contract has expired. How soon after the contract expires would depend on the Organization's business and legal needs.

9.3 Retention Policy

To assist the Organization in complying with the retention principle under the PDPA, the Organization has designed and implemented a specific document retention policy. Please refer to CP-C0237 – Records Retention Policy for more details.

10. TRANSFER LIMITATION OBLIGATION / PRINCIPLE

10.1 Introduction

10.1.1 Pursuant to the transfer out principle under the PDPA, the Organization must not transfer personal data to a country or territory outside Singapore unless it ensures that the recipient organization is bound by legally enforceable obligations to provide the transferred personal data with a level of protection that is comparable to the protection under the PDPA.

10.1.2 Consent to such transfers (unless an exception under the PDPA applies) should be obtained from the individuals whose personal data is to be transferred.

10.2 Transferring Personal Data Outside Of Singapore

10.2.1 In light of the transfer out principle, the Organization has put in place policy(ies)/procedure(s)/practice(s) to deal with when and how personal data may be transferred out of Singapore. This includes the Organization executing an agreement with the recipient organization to deal with the data transfer. You must not transfer personal data to any party outside of Singapore until the recipient organization has entered into and agreed to be bound by such an agreement and the individual whose personal data is to be transferred has consented to the same (unless an exception to the consent principle applies). Check with the Organization's Data Protection Officer or the Organization's management if you are uncertain on whether there is such an arrangement in place when you are transferring personal data.

10.2.2 The transfer out principle would apply equally regardless of whether the overseas recipient is a group company or a third party organization. Be aware that transferring personal data out of Singapore is not limited to the physical transfer of personal data outside of Singapore.

11. THE ACCOUNTABILITY OBLIGATION

11.1 Being Transparent And Accountable

11.1.1 All personal data within the possession or control of the Organization is the Organization's responsibility and you must always ensure that you handle such personal data in full compliance with the PDPA.

11.1.2 The Organization expects all employees to fully comply with this Singapore Policy and the PDPA and in this regard, the Organization shall be, and expects its employees to be transparent and accountable with regard to how it collects, uses and discloses an individual's personal data.

11.1.3 The Organization has made available to the public the business contact information of its Data Protection Officer.

11.1.4 Complaint Process or Request for Information

11.1.5 The Organization is also required to deal with complaints from any party with respect to how it has dealt with the PDPA and its activities in relation to personal data. Anyone could potentially seek information from the Organization as to the policies and practices that the Organization has put in place to meet its obligations under the PDPA.

11.1.6 Such complaints or request for information can come in any form, such as by way of an email, face to face communication, telephone call etc. It could be from an individual customer, a staff of a corporate customer, or a member of the public etc. When you receive a complaint or a request for information (whether in writing or otherwise), you must act on such complaint by immediately notifying the Data Protection Officer.

12. DATA BREACH NOTIFICATION OBLIGATION / PRINCIPLE

12.1 Introduction

12.1.1 This obligation/principle is where the Organization needs to notify the PDPC and/or the affected individual upon a notifiable data breach occurring.

12.1.2 A data breach is when there has been (a) unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or (b) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

12.1.3 If there is any doubt as to whether a data breach has occurred, the Data Protection Officer should be consulted immediately.

12.1.4 Not all data breaches are notifiable to the PDPC and/or the affected individual. A data breach only becomes notifiable as set out below.

12.2 Notifiable Data Breach

12.2.1 A data breach is notifiable if :

(a) it results in or is likely to result in, significant harm to the affected individual. Such a data breach must be notified to both the PDPC and the affected individual.

(b) it is or is likely to be of a significant scale (i.e. affects the personal data of 500 or more individuals). The Organization must notify the PDPC of such data breaches.

12.3 Notification Process

12.3.1 Refer to the Data Breach Management Plan for full details on what you need to do in recognizing and dealing with a data breach, and on the notification process. You are required to read and understand the Data Breach Management Plan.

13. DO NOT CALL REGISTRY

13.1.1 Under the PDPA, a Do Not Call (i.e. DNC) regime/framework has been established to enable individuals to register their Singapore telephone number(s) with the DNC registry if they do not wish to receive marketing messages through their Singapore telephone number.

13.1.2 The DNC regime/framework applies to all manifestations or forms of messages, whether in sound, text, visual or other form. It would therefore include messages such as Short Messaging Service ("**SMSes**") messages and Multimedia Messaging Service ("**MMSes**")

messages, voice calls and any data applications which use a Singapore telephone number. A voice call includes a call that involves a recorded or synthetic voice.

13.1.3 The DNC regime will impose restrictions on :

(a) marketing telephone or voice calls;

(b) marketing text messages (SMSes and MMSes); and/or

(c) marketing fax messages,

that are sent to a Singapore telephone number. It can be a Singapore landline, a Singapore mobile phone number, or a Singapore fax number, whether residential or business lines. The DNC regime/framework will however not apply to telephone numbers of other countries such as a Thailand telephone number or an Indonesian telephone number. Under the DNC regime/framework, a Do Not Call registry ("**DNC Registry**"), comprising of three (3) registers, is maintained by the PDPC, as follows :

(a) one for marketing telephone or voice calls;

(b) another for marketing text messages (SMSes and MMSes); and

(c) a third for fax messages,

(the "**DNC Registers**").

13.1.4 Pursuant to the DNC regime/framework, certain kinds of messages will be subject to certain conditions. These messages would essentially be messages of a marketing nature ("**Marketing Messages**"). A "Marketing Message" is very broadly defined in the PDPA and can include a message (a voice call, an SMS/MMS or a fax) where the purpose of the message, or one of the purposes of the message, is:

(a) to offer to supply goods or services;

(b) to advertise or promote goods or services; or

(c) to offer to provide a business opportunity or an investment opportunity.

14.2 <u>The Prohibitions under the Do Not Call regime/framework</u>

14.2.1 Three (3) key requirements or prohibitions apply to all Marketing Messages:

(a) The "Requirement to Check with the DNC Registry";

(b) The "Requirement to provide Contact Information"; and

(c) The "Voice Call Calling Line Identity Prohibition".

14.3 <u>Requirement to Check with the DNC Registry</u>

14.3.1 The Requirement to Check with the DNC Registry is as follows :

14.3.2 Before you send a Marketing Message to a Singapore telephone number, you must strictly comply with the following :

(a) within 21 days prior to sending the Marketing Message have checked with the DNC Registry under the PDPC on whether that Singapore telephone number has been registered with the relevant DNC Register (depending on whether a fax, SMS or voice call is intended to be sent/made); and

(b) only if there is confirmation from the DNC Registry that that Singapore telephone number is not registered with the relevant DNC Register, can that organization or person then send the Marketing Message to that Singapore telephone number via the mode of communication for which the Singapore telephone number has not been registered.

14.3.3 If that Singapore telephone number is found to be registered, that organization or person must not send the Marketing Message to that Singapore telephone number.

14.4 The Requirement to provide Contact Information

14.4.1 Any Marketing Message must contain clear and accurate information :

(a) identifying the organization that sent or authorised the sending of the Marketing Message;

(b) on how the recipient of the Marketing Message can readily contact the sender; and

(c) that is to be valid for at least 30 days after the recipient receives the Marketing Message.

14.5 The Voice Call Calling Line Identity Prohibition

14.5.1 If the Marketing Message is in the form of a voice call/telephone call made to the recipient, the calling line identity must not be concealed from the recipient and the recipient must be able to see the calling line identity of the sender of the said call. "**Calling line identity**" means the telephone number or information identifying the sender.

14.5.2 In this regard, if a voice call/telephone call is made, the recipient must be able to see the actual telephone number of the sender and the sender information on his telephone/mobile phone must not read as 'Blocked' or 'Private Number' or any other words to that effect.