## 12 The Consent Obligation

12.1 Section 13 of the PDPA prohibits organisations from collecting, using or disclosing an individual's personal data unless the individual gives, or is deemed to have given, his consent for the collection, use or disclosure of his personal data. This requirement to obtain consent does not apply where collection, use or disclosure of an individual's personal data without consent is required or authorised under the PDPA or any other written law. This obligation to obtain the individual's consent is referred to in these Guidelines as the Consent Obligation.

12.2 Sections 14 to 17 of the PDPA deal with a number of issues relating to the Consent Obligation, which are explained below.

12.3 An important point to note is that the PDPA does not affect existing legal or regulatory requirements that organisations have to comply with. Organisations may collect, use and disclose (as the case may be) personal data without the individuals' consent if required or authorised to do so under the PDPA or other written law, although the organisations may need to comply with other requirements of the Data Protection Provisions which are not inconsistent with its obligations under written law. For more information on this, please refer to the section on Existing Rights, Obligations and Uses.

Obtaining consent from an individual

12.4 Section 14(1) of the PDPA states how an individual gives consent under the PDPA. In particular, an individual has not given consent unless the individual has been notified of the purposes for which his personal data will be collected, used or disclosed and the individual has provided his consent for those purposes. If an organisation fails to inform the individual of the purposes for which his personal data will be collected, used and disclosed, any consent given by the individual would not amount to consent under section 14(1). Further details on the organisation's obligation to notify the individual are explained in the section on the "Notification Obligation".

12.5 Consent can be obtained in a number of different ways. As good practice, an organisation should obtain consent that is in writing or recorded in a manner that is accessible for future reference, for example, if the organisation is required to prove that it had obtained consent.

12.6 An organisation may also obtain consent verbally although it may correspondingly be more difficult for an organisation to prove that it had obtained consent. For such situations, it would be prudent for the organisation to, minimally, document the consent in some way, for example, by noting the fact that oral consent was provided by an individual for certain purposes, together with the date and time of such

consent.

Obtaining consent verbally

12.7 In situations where the organisation cannot conveniently obtain consent from an individual in writing, it may choose to obtain verbal consent. However, organisations should note that in cases of dispute it may be more challenging to prove that verbal consent had been given if there is no other supporting evidence.

12.8 As good practice, organisations can consider adopting the following practices in cases when consent is obtained verbally:

a) Confirm the consent in writing with the individual (which may be in electronic form or other form of documentary evidence); or

b) Where appropriate in the circumstances, make a written note (which may be in electronic form or other form of documentary evidence) of the fact that an individual had provided verbal consent.

Example:

An individual wishes to sign up for certain services with a service provider over the telephone. The service provider may request for the individual's consent to the collection and use of his personal data for the service provider's purposes and obtain the personal data from the individual over the telephone.

It would be good practice for the service provider to subsequently contact the individual and confirm his consent in writing, for example, by sending an email to the individual setting out the personal data provided by the individual and recording his consent to collection, use and disclosure by the service provider for the service provider's purposes (which may be set out in its terms and conditions and/or other information provided in the email).

12.9 Organisations that wish to rely on the individual's consent to send specified messages to Singapore telephone numbers should note that the relevant defence in the Do Not Call Provisions requires such consent to be clear and unambiguous consent to the sending of the specified message to that Singapore telephone number, evidenced in written or other accessible form. For this purpose, verbal consent would be insufficient unless it can be recorded in a form which is accessible for subsequent reference. Please refer to Chapters 7 and 8 of the Advisory Guidelines on the Do Not Call Provisions for more details.

Failure to opt out

12.10 The Commission notes that there are various means of obtaining an individual's consent to the collection, use and disclosure of his personal data for a specified purpose. In some cases, organisations might adopt the opt out avenue to obtain consent, for example, by deeming that an individual has given his consent through inaction on his part. In general, the Commission notes that failure to opt out may be due to other reasons than the individual's desire to give consent. The Commission's view is that a failure to opt out will not be regarded as consent in all situations. Rather, whether or not a failure to opt out can be regarded as consent will depend on the actual circumstances and facts of the case. The opt out method of obtaining consent also has many variants, and depending on its implementation, could be more or less likely to constitute consent.

> Example:
>
> Retailer A has collected personal data from its customers for the purpose of delivering products purchased by the customers. It subsequently mails a flyer to the customers which states that a customer would have consented to the disclosure of his personal data to Company Z to market the products of Company Z unless the customer writes back to the retailer to opt out by a certain date. Company Z receives no response from the customer. In this case, the customer's inaction is unlikely to signify consent since it may be due to other reasons not related to a desire to consent (e.g. not having opened the mailbox or read the flyer).
>
> Retailer B puts up a sign informing customers who are interested to join their membership programme to obtain an application form from a shelf next to the counter, fill it out, and drop the completed form into an unmanned box next to the shelf. A line in the form with an accompanying tick box states clearly "tick here if you do not wish your personal data to be provided to Company Z to market Company Z's products". The last field of the form requires the customer to provide his signature. The customer signed the form without putting a tick in the tick box and drops the completed form into the box. In this case, the customer is more likely to have given his consent to the disclosure of his personal data to Company Z for Company Z's marketing purposes.

12.11 The Commission would recommend that organisations obtain consent from an individual through a positive action of the individual to consent to the collection, use and disclosure of his personal data for the stated purposes. If an organisation intends to adopt the opt out approach in seeking consent, the organisation should consider the risks that it may not have satisfied the Notification Obligation and Consent Obligation.

12.12 In relation to the Do Not Call Provisions where an organisation wishes to rely on the clear and unambiguous consent of an individual to the sending of the specified message to a Singapore telephone number to send a specified message to a Singapore telephone number registered on the Do Not Call Registry, the Commission will generally not view the mere failure to opt out as clear and unambiguous consent given by an individual. Organisations that wish to send telemarketing messages to individuals regardless of the registrations on the Do Not Call Registry should obtain a clear indication from the individual that he has opted to receive the telemarketing message, i.e. opt in consent.

Obtaining consent from a person validly acting on behalf of an individual

12.13 Section 14(4) of the PDPA provides that consent may be given, or deemed to have been given, by any person validly acting on behalf of the individual for the collection, use or disclosure of the individual's personal data. Regulations issued under the PDPA will also provide for some specific situations in which an individual person may give consent on behalf of another.

12.14 In order to obtain consent from a person validly acting on behalf of an individual, the person would similarly have to be notified of the purposes for which the individual's personal data will be collected, used and disclosed and the person must have given consent for those purposes on behalf of the individual. The following sections elaborate on when consent is not validly given and deemed consent would also apply.

When consent is not validly given

12.15 Section 14(2) of the PDPA sets out additional obligations that organisations must comply with when obtaining consent. This subsection provides that an organisation providing a product or service to an individual must not, as a condition of providing the product or service, require the individual to consent to the collection, use or disclosure of his personal data beyond what is reasonable to provide the product or service. The subsection also prohibits organisations from obtaining or attempting to obtain consent by providing false or misleading information or using deceptive or misleading practices.

12.16 Section 14(3) provides that any consent obtained in such circumstances is not valid. Hence an organisation may not rely on such consent, and if it collects, uses or discloses personal data in such circumstances, it would have failed to comply with the Consent Obligation.

12.17 For the avoidance of doubt, organisations may collect, use or disclose personal data for purposes beyond those that are reasonable for providing the product or service

to the individual by obtaining the individual's consent in accordance with the PDPA, so long as organisations do not make it a condition of providing the product or service.

> Example:
>
> Sarah wants to signs up for a spa package. The terms and conditions include a provision that the spa may share her personal data with third parties, including selling her personal data to third party marketing agencies. Sarah does not wish to consent to such a disclosure of her personal data and requests the spa not to disclose her personal data to third party marketing agencies. The spa refuses to act on her request and informs her that the terms and conditions are standard, and that all customers must agree to all the terms and conditions. Sarah is left either with the choice of accepting all the terms and conditions (i.e. giving consent for use and disclosure of her data as described) or not proceeding with the sign up. In this case, even if Sarah consents to the disclosure of her data to third party marketing agencies, the consent would not be considered valid since it is beyond what is reasonable for the provision of the spa's services to its customers, and the spa had required Sarah's consent as a condition for providing its services.
>
> Instead of requiring Sarah to consent to the disclosure and sale of her personal data to third parties as a condition of providing the service, the spa should separately request Sarah's consent to do so. That is, Sarah should be able to sign up for the spa package without having to consent to the disclosure and sale of her personal data to third parties. The spa is then free to ask Sarah if she would consent, and if she does, would be considered to have obtained valid consent.

12.18 Section 14(2)(a) may not prohibit certain situations in which an organisation may seek to require consent. For example, organisations may provide offers, discounts or lucky draw opportunities to individuals that are conditional on the collection, use or disclosure of their personal data for specified purposes. In any event, organisations are reminded that their practices would be subject to other requirements of the Data Protection Provisions including, in particular, the requirement that the organisation's purposes must be what a reasonable person would consider appropriate in the circumstances.

12.19 When collecting personal data through a form, it is good practice for organisations to indicate which fields that collect personal data are compulsory and which are optional, and to state the purposes for which such personal data will be collected, used and/or disclosed.

12.20 It follows from section 14(2)(a) that an organisation may require an individual to consent to the collection, use or disclosure of his personal data as a condition of providing a product or service where it is reasonably required in order to provide the

product or service. For more information on requiring consent for the collection, use or disclosure of personal data for marketing purposes, please refer to the Advisory Guidelines on Requiring Consent for Marketing Purposes.

12.21 In particular, where an organisation would be unable to provide the product or service to the individual if the individual did not consent (or withdrew consent) to the collection, use or disclosure of his personal data for that purpose, the organisation should give due consideration to whether the personal data requested is necessary or integral to providing the product or service.

> Example:
>
> An individual wishes to obtain certain services from a telecom service provider and is required by the telecom service provider to agree to its terms and conditions for provision of the services. The telecom service provider can stipulate, as a condition of providing those services, that the individual agrees to the collection, use and disclosure of specified items of personal data which is reasonably required by the telecom service provider to supply the subscribed services to the individual. Such items of personal data may include the name and address of the individual as well as personal data collected in the course of providing the services such as the individual's location data.

12.22 Section 14(2)(b) addresses the situation where an organisation obtains or attempts to obtain consent by providing false or misleading information or using misleading and deceptive practices. Such practices may include situations where the purposes are stated in vague or inaccurate terms, in an illegible font or placed in an obscure area of a document or a location that is difficult to access.

Deemed consent

12.23 Section 15 of the PDPA addresses two situations in which an individual may be deemed to consent even if he has not actually given consent. The first is where an individual voluntarily provides his personal data for a purpose. Under section 15(1), an individual is deemed to consent to the collection, use and disclosure of his personal data for a purpose if the individual voluntarily provides the personal data to the organisation for that purpose and it is reasonable that the individual would do so.

Example:

Sarah makes a visit to a spa for a facial treatment. After the treatment is completed, she makes her way to the cashier to make payment. The cashier tells her that the facial will cost her $49.99. She hands over her credit card to the cashier for the purpose of making payment. The cashier need not ask for Sarah's consent to collect, use or disclose her credit card number and any other related personal data (e.g. name on credit card) required to process the payment transaction.

Sarah would be deemed to have consented to the collection, use and disclosure of her credit card number and other related personal data for processing of the payment as she voluntarily provided the personal data and it is reasonable that Sarah would provide the personal data to pay for her facial. Sarah's deemed consent would extend to all other parties involved in the payment processing chain who collect or use Sarah's personal data. These parties could include, for example, Sarah's bank, the spa's bank and its processers and the payment system provider.

12.24 For deemed consent under section 15(1) to apply, the onus would be on the organisation involved to ensure that the individual was aware of the purpose for which his personal data would be collected, used or disclosed.

Example:

Sarah calls a taxi operator's hotline to book a taxi. The customer service officer asks for her name and number in order to inform her of the taxi number, which Sarah provides voluntarily. Sarah is deemed to have consented to the taxi company using her name and number to call or text her when her taxi arrives.

However, if the taxi operator runs a limousine service and wanted to use Sarah's information to market this service to her, Sarah would not be deemed to have consented to the use of her personal data for this purpose. This is because Sarah provided her personal data for the purpose of booking a taxi for a single trip, and not for the purpose of receiving marketing information about the limousine service.

12.25 An individual may sometimes be regarded as voluntarily providing personal data where the individual takes some action that allows the data to be collected, without actually providing the data himself. Hence the onus will be on the organisation involved to establish that the individual wanted to provide his personal data and took the action required for it to be collected by the organisation.

Example:

Sarah goes for a medical check-up at a clinic. For the purposes of the check-up, the clinic will be conducting a series of tests which include measuring her height and weight. Sarah is aware that such tests will be conducted as the clinic has provided this information on the registration form that Sarah filled out and submitted prior to the tests. Sarah will be deemed to have consented to the collection of her personal data by submitting to the tests even though she did not directly provide the data to the clinic.

12.26 Section 15(1) also requires that it be reasonable for the individual to have voluntarily provided his personal data. Hence, consent will not be deemed to have been given where the individual could not reasonably be expected in the circumstances to have provided his or her personal data for a purpose.

12.27 The second situation in which consent may be deemed is where an individual consents to the disclosure of his personal data by one organisation ("A") to another ("B"). Under section 15(2), if an individual gives or is deemed to have given consent for disclosure of his personal data by A to B for a purpose, the individual is deemed to consent to the collection of his personal data by B for that purpose.

Example:

In an example above, Sarah was deemed to have consented to a facial company collecting, using or disclosing her credit card details to process the payment for her facial. In the course of processing the payment, her credit card details are transmitted to the bank who handles the payment. Since Sarah is deemed to consent to the disclosure of her credit card details by the facial company to the bank, she is also deemed to consent to the collection of her credit card details by the bank for the purpose of processing the payment to the facial company.

12.28 Although organisations may rely on deemed consent instead of obtaining actual consent from the individual, it is good practice for an organisation to review its business processes to determine the situations where it should obtain actual consent instead of seeking to rely on deemed consent. Relying on deemed consent requires an organisation to be able to establish the following:

a) an individual voluntarily provided his personal data;

b) the individual was aware of the purpose for which the personal data was provided; and

c) the circumstances are such that it is reasonable for the individual to have

provided his personal data.

12.29 In some situations, as in the examples noted above, it may be clear that the deemed consent provision would apply. However, if it is not clear whether the deemed consent provision applies, obtaining consent from the individual would avoid disputes where an individual claims that he did not consent to the collection of his personal data for a purpose and that he did not voluntarily provide personal data for the purpose.

Obtaining personal data from third party sources with the consent of the individual

12.30 As noted above, there are two situations in which organisations may obtain personal data about an individual with the consent of the individual but from a source other than the individual (a "third party source"). These are, in brief:

a) where the third party source can validly give consent to the collection, use and disclosure of the individual's personal data (under section 14(4) of the PDPA); or

b) where the individual has consented, or is deemed to have consented, to the disclosure of his or her personal data by the third party source (under section 15(2) of the PDPA).

12.31 Examples of the above situations could be a referral from an existing customer, where an individual has allowed another (the existing customer) to give consent to the collection of his personal data by the organisation, or the purchase of a database containing personal data from a database reseller who had obtained consent for the disclosure of the personal data.

12.32 There could also be cases, especially with organisations that operate in a group structure, where one organisation in the group has validly obtained consent to the collection, use and disclosure of an individual's personal data for the purposes of other organisations in the corporate group. For example, when an individual subscribes to a service offered by one organisation in a corporate group, the organisation could have obtained the individual's consent to the collection, use and disclosure of his personal data for the purposes of marketing and promoting the products and services of that organisation and the other companies within the corporate group.

12.33 An organisation collecting personal data from a third party source is required to notify the source of the purposes for which it will be collecting, using and disclosing the personal data (as applicable). For further details on this, please refer to the section on the "Notification Obligation".

Exercising appropriate due diligence when obtaining personal data from third party sources

12.34 Organisations obtaining personal data from third party sources should exercise the appropriate due diligence to check and ensure that the third party source can validly give consent for the collection, use and disclosure of personal data on behalf of the individual (under section 14(4)) or that the source had obtained consent for disclosure of the personal data (under section 15(2)). In the event the third party source could not validly give consent or had not obtained consent for disclosure to the collecting organisation, but concealed this from the collecting organisation, the actions taken by the collecting organisation to verify such matters before collecting the personal data from the third party source would be considered a possible mitigating factor by the Commission should there be a breach of the PDPA relating to such collection or the collecting organisation's use or subsequent disclosure of the personal data.

12.35 In exercising appropriate due diligence to verify that a third party source ("B") can validly give consent or has obtained consent from the individual concerned, organisations ("A") may adopt one or more of the following measures appropriate to the circumstances at hand:

a) Seek an undertaking from B through a term of contract between A and B that the disclosure to A for A's purposes is within the scope of the consent given by the individual to B;

b) Obtain confirmation in writing from B;

c) Obtain, and document in an appropriate form, verbal confirmation from B; or

d) Obtain a copy of the document(s) containing or evidencing the consent given by the individuals' concerned to B to disclose the personal data[10].

Example:

Sarah provides the personal data of her friend Jane to the sales consultant at her spa as part of a member's referral programme the spa is running. Before recording Jane's personal data, the sales consultant asks Sarah a few questions to determine if Jane had been informed of the purposes for which her personal data is being disclosed to and used by the spa, and if Jane had indeed provided her consent.

[10] The Commission notes that this may not always be possible or practical, e.g. in situations where such documents contain personal data which cannot be disclosed to A.

After obtaining verbal confirmation from Sarah in the affirmative to those questions, the sales consultant proceeded to collect Jane's personal data. The sales consultant is likely to have exercised appropriate due diligence in this situation.

As good practice, when contacting Jane for the first time, the sales consultant should inform Jane that her personal data was disclosed by Sarah and verify that Jane had provided consent to do so.

Obtaining personal data from third party sources without the consent of the individual

12.36 An organisation ("A") may collect personal data from a third party source ("B") (as described in the previous section) without the consent of the individual in the circumstances described in the Second Schedule to the PDPA. These circumstances include, for example, where:

a) the collection is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual;

b) the personal data is publicly available; and

c) the collection is necessary for evaluative purposes.

12.37 If B is an organisation that is required to comply with the PDPA, it would only be able to disclose the personal data without the consent of the individual in one of the circumstances set out in the Fourth Schedule to the PDPA. These circumstances include, for example, where:

a) the disclosure is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual;

b) the personal data is publicly available; and

c) the disclosure is for the purpose of contacting the next-of-kin or a friend of any injured, ill or deceased individual.

12.38 As consent of the individual is not required, A is not required to verify that B had notified the individual of the purposes for which his personal data would be collected, used and disclosed and obtained the individual's consent. However, B would need to know the purpose for which A is collecting the personal data in order to determine if its disclosure of the data to the organisation would be in accordance with the PDPA. The Data Protection Provisions thus require A to inform B of its

purposes. In particular, section 20(2)[11] of the PDPA requires A to provide B with sufficient information regarding its purpose for collecting the personal data to allow B to determine whether disclosure would be in accordance with the PDPA.

Withdrawal of consent

12.39 Section 16 of the PDPA provides that individuals may at any time withdraw any consent given or deemed to have been given under the PDPA in respect of the collection, use or disclosure of their personal data for any purpose by an organisation.

12.40 Section 16 sets out a number of requirements that must be complied with by either the individual or the organisation in relation to a withdrawal of consent. In brief, they are:

a) the individual must give reasonable notice of the withdrawal to the organisation (section 16(1));

b) on receipt of the notice, the organisation must inform the individual of the likely consequences of withdrawing consent (section 16(2));

c) an organisation must not prohibit an individual from withdrawing consent, although this does not affect any legal consequences arising from such withdrawal (section 16(3)); and

d) upon withdrawal of consent, the organisation must cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless the collection, use or disclosure of the personal data without consent is required or authorised under the PDPA or any other written law (section 16(4)).

Organisations must allow and facilitate the withdrawal of consent

12.41 In general, organisations must allow an individual who has previously given (or is deemed to have given) his consent to the organisation for collection, use or disclosure of his personal data for a purpose to withdraw such consent by giving reasonable notice. In this regard, considerations for whether the individual has given reasonable notice would include the amount of time needed to give effect to the

[11] Section 20(2) states that – "An organisation, on or before collecting personal data about an individual from another organisation without the consent of the individual, shall provide the other organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with this Act."

withdrawal of consent and the manner in which notice was given.

12.42 The Commission considers that it would be difficult to take a one-size-fits-all approach and prescribe a specific time frame for reasonable notice to be given. However, as a general rule of thumb, the Commission would consider a withdrawal notice of at least ten (10) business days from the day the organisation receives the withdrawal notice, to be reasonable notice. Should an organisation require more time to give effect to a withdrawal notice, it is good practice for the organisation to inform the individual of the time frame by which the withdrawal of consent will take effect.

12.43 In order to enable and facilitate withdrawal, organisations are advised to make an appropriate consent withdrawal policy that is clear and easily accessible to the individuals concerned. This withdrawal policy should, for example:

a) advise the individuals on the form and manner to submit a notice to withdraw their consent for specific purposes;

b) indicate the person to whom, or the means by which, the notice to withdraw consent should be submitted; and

c) distinguish between purposes necessary and optional to the provision of the products/services (that may include the service of the existing business relationship). Individuals must be allowed to withdraw consent for optional purposes without concurrently withdrawing consent for the necessary purposes.

12.44 Organisations should not have inflexible consent withdrawal policies that seek to restrict or prevent individuals from withdrawing consent in accordance with the PDPA.

12.45 An organisation must not prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual himself. For example, if an organisation requires certain personal data from an individual in order to fulfil a contract with the individual to provide products or services, it may not stipulate as a term of the contract that the individual cannot withdraw consent to the collection, use or disclosure of the individual's personal data for the purposes of the contract. If the individual subsequently withdraws consent to his personal data in a manner which makes it impossible for the contract to be fulfilled, any legal consequences arising out of such withdrawal would not be affected.

Example:

An individual wishes to obtain certain services from a telecom service provider, Operator X and is required by the telecom service provider to agree to its terms and conditions for provision of the services. Operator X can stipulate as a condition of providing the services that the individual agrees to the collection, use and disclosure of specified types of personal data by the organisation for the purpose of supplying the subscribed services. Such types of personal data may include the name and address of the individual as well as personal data collected in the course of providing the services such as the individual's location data. The individual provides consent for those specified types of personal data but subsequently withdraws that consent.

The withdrawal of consent results in Operator X being unable to provide services to the individual. This would in turn entail an early termination of the service contract. Operator X should inform the individual of the consequences of the early termination, e.g. that the individual would incur early termination charges.

12.46 If an individual has withdrawn his earlier consent to the collection, use or disclosure of his personal data by an organisation, but subsequently provides fresh consent to the organisation, the organisation may collect, use or disclose his personal data within the scope of the fresh consent that he subsequently provided.

Example:

Peter withdraws his consent to Organisation ABC to send him marketing messages via e-mail, and accordingly, ABC ceases to do so.

A few months later, Peter decides that he now wishes to receive marketing messages via e-mail from ABC and provides his consent for ABC to send him marketing messages via e-mail. ABC may now rely on the consent provided by Peter to send him marketing messages via e-mail again, notwithstanding that Peter had previously withdrawn his consent.

Effect of a withdrawal notice

12.47 In determining the effect of any notice to withdraw consent, the Commission will consider all relevant facts of the situation. This could include but is not limited to matters like:

a) the actual content of the notice of withdrawal;

b) whether the intent to withdraw consent was clearly expressed; and

c) the channel through which the notice was sent.

12.48 In cases where an organisation provides a facility for individuals to withdraw consent (e.g. by clicking on an "unsubscribe" link within an e-mail), the organisation should clearly indicate the scope of such withdrawal. The organisation is also encouraged to inform individuals of how they may withdraw consent for matters outside the scope of such withdrawal. In facilitating any notice to withdraw consent, an organisation should act reasonably and in good faith.

> Example:
>
> Organisation ABC has obtained consent from Joan to send her marketing messages via e-mail and fax.
>
> ABC sends Joan an e-mail informing her of the latest in-store promotion, and included a link for her to unsubscribe:
>
> "*If you wish to stop receiving marketing messages from ABC via e-mail, please click on the link 'unsubscribe'. If you wish to stop receiving marketing messages from ABC via other channels, please send us an e-mail at dpo@abc.org.*"
>
> Joan clicks on the 'unsubscribe' link and is directed to a website which states:
>
> "*You have unsubscribed successfully from e-mail marketing messages from ABC.*"
>
> Joan would be considered to have withdrawn consent to receive marketing messages sent by e-mail only. If Joan writes to ABC stating her intention to withdraw consent from receiving marketing messages via fax, ABC must facilitate the withdrawal of consent.

*Where a withdrawal notice for marketing is kept general*

12.49 Typically, where the withdrawal notice for marketing contains a general withdrawal message, i.e. it is not clear as to the channel of receiving marketing messages for which consent is withdrawn, the Commission will consider any withdrawal of consent for marketing sent via a particular channel to only apply to all messages relating to the withdrawal sent via that channel. Please see the example below for more details.

> Example:
>
> Organisation ABC has obtained consent from Sally to send her marketing messages via e-mail and fax.

ABC sends Sally an e-mail informing her of the latest in-store promotion, and included a link for her to unsubscribe:

"*If you wish to stop receiving marketing messages from ABC, please click on the link 'unsubscribe'.*"

Sally clicks on the 'unsubscribe' link and is directed to a website which states:

"*You have unsubscribed successfully.*"

As the withdrawal notice is general and does not specify the channel of receiving marketing messages for which consent is withdrawn, Sally would be considered to have withdrawn consent to receive marketing messages sent by e-mail only.

12.50 Where relevant, organisations should consider how the withdrawal notice impacts both consent obtained under the Data Protection Provisions and the Do Not Call Provisions. Please refer to Chapter 8 of the Advisory Guidelines on the Do Not Call Provisions for more details on withdrawal of consent under the Do Not Call Provisions.

Actions organisations must take upon receiving a notice of withdrawal

12.51 Once an organisation has received from an individual a notice to withdraw consent, the organisation should inform the individual concerned of the likely consequences of withdrawing his consent, even if these consequences are set out somewhere else, e.g. in the service contract between the organisation and the individual.

12.52 Consequences for withdrawal of consent could simply be that the organisation would cease to collect, use or disclose the individual's personal data for the purpose specified by the individuals. In other cases, the organisation may not be able to continue providing services to the individual or there may be legal consequences.

12.53 With regard to personal data that is already in an organisation's possession, withdrawal of consent would only apply to an organisation's continued use or future disclosure of the personal data concerned. Upon receipt of a notice of withdrawal of consent, the organisation must cease to collect, use or disclose the individual's personal data, and inform its data intermediaries and agents about the withdrawal and ensure that they cease collecting, using or disclosing the personal data for the various purposes.

12.54 Apart from its data intermediaries and agents, an organisation is not required to inform other organisations to which it has disclosed an individual's personal data of the individual's withdrawal of consent. This does not affect the organisation's obligation to provide, upon request, access to the individual's personal data in its

possession or control and information to the individual about the ways in which his personal data may have been disclosed. Hence the individual may find out which other organisations his personal data may have been disclosed to and give notice to withdraw consent to those other organisations directly.

12.55 Although an individual may withdraw consent for the collection, use, or disclosure of his personal data, the PDPA does not require an organisation to delete or destroy the individual's personal data upon request. Organisations may retain personal data in their documents and records in accordance with the Data Protection Provisions. For more information on this, please refer to the section on the "Retention Limitation Obligation".

Example:

Andy had previously given his consent to Y Electronics to collect, use and disclose his contact details (which form part of his personal data) for the purpose of providing him with marketing information and promotional offers on computers and other IT products. Y Electronics discloses Andy's contact details to its outsourced marketing agent and some other third party companies offering computers and other IT products to fulfil that purpose. Andy changes his mind and submits a notice to withdraw the consent he gave to Y Electronics for the purpose of marketing computers and other IT products.

Y Electronics is required to notify Andy of the consequences of his withdrawal, for example, that:

a) Y Electronics and its marketing agents will cease to send information on computer and IT products to Andy;

b) Y Electronics will cease to disclose Andy's personal data to any third party; and

c) Y Electronics will cease using Andy's contact details for marketing computer and IT products and will instruct its outsourced marketing agent likewise (so that it will cease sending marketing information to Andy).

However, Y Electronics will not be required to inform the third party companies to which it disclosed Andy's contact details, and Andy will have to approach those companies to withdraw consent if he wishes to do.

The withdrawal of consent also does not affect Y Electronics' ability to retain Andy's personal data that it requires for legal or business purposes. For example, Y Electronics may still retain Andy's personal data in its database for the purpose of servicing an ongoing warranty, or records of his purchases that are necessary for audit purposes.

Exceptions to the Consent Obligation

12.56 Section 17 of the PDPA permits the collection, use and disclosure of personal data without consent (and, in the case of collection, from a source other than the individual) only in the circumstances provided in the Second Schedule (Collection of personal data without consent), Third Schedule (Use of personal data without consent) and Fourth Schedule (Disclosure of personal data without consent) to the PDPA respectively. These exceptions to the Consent Obligation do not affect rights or obligations arising under any other law. Hence, even if an exception applies under the PDPA, organisations are required to comply with their other legal obligations, for example, to protect confidential information or other contractual obligations.

Publicly available data

12.57 One significant exception in the Second, Third and Fourth Schedules to the PDPA relates to personal data that is publicly available. The term "publicly available" is defined in section 2(1) of the PDPA and refers to personal data (about an individual) that is generally available to the public, including personal data which can be observed by reasonably expected means at a location or an event at which the individual appears and that is open to the public.

12.58 The explanation "generally available to the public" refers to the commonly understood meaning of the term "publicly available". Personal data is generally available to the public if any member of the public could obtain or access the data with few or no restrictions. In some situations, the existence of restrictions may not prevent the data from being publicly available.

12.59 For example, if personal data is disclosed to a closed online group but membership in the group is relatively open and members of the public could join with minimal effort, then the disclosure may amount to making the data publicly available. Conversely, if personal data is disclosed to a close circle of the individual's family and friends or it is inadvertently disclosed to a single member of the public who is not personally known to the individual concerned, the disclosures may not make the personal data publicly available.

Example:

Alan is a member of an online social network that is open to the public[12]. His membership profile which is publicly searchable lists his name, date of birth and the university at which he is currently enrolled. Alan also regularly updates his profile picture. The data (including pictures of him) which Alan has shared on this online social network is very likely to be personal data that is publicly available, since any other user of the social network would be able to gain access to the data, even if they accessed his profile page by accident and any member of public may join the online social network.

Bob is a member of the same social network. However, Bob's membership profile is only accessible by a few users who are personally known to him and to whom he has granted permission to access his profile. Bob has also placed restrictions on the re-posting of his profile. The personal data on Bob's membership profile is less likely to be considered publicly available since access to the data is strictly limited.

12.60 The Commission recognises that personal data that is publicly available at one point in time may, for various reasons, no longer be publicly available after that time. For example, users of social networking sites may change their privacy settings from time to time, which would have an impact on whether their personal data would be considered publicly available.

12.61 The Commission recognises that it would be excessively burdensome for organisations intending to use or disclose publicly available personal data without consent to constantly verify that the data remains publicly available, especially in situations where the use or disclosure happens some time after the collection of the personal data. Hence, the Commission will take the position that so long as the personal data in question was publicly available at the point of collection, organisations will be able to use and disclose personal data without consent under the corresponding exceptions, notwithstanding that the personal data may no longer be publicly available at the point in time when it is used or disclosed.

12.62 Publicly available personal data also includes a category of personal data that is specifically included in the definition, that is, personal data observed in public. For this to apply, there are two requirements relating to how and where the personal

[12] The Commission notes that organisations which operate websites or applications may subject their users to a standard set of terms and conditions, which could include reserving the right to make the personal data of users publicly available (or disclose the personal data in specified ways) that could be contrary to their users' personal preferences to restrict access to their personal data. In such cases, whether the organisation had obtained valid consent from users would depend on whether the organisation had obtained consent in accordance with the PDPA, for example whether it had fulfilled the Consent, Purpose Limitation and Notification Obligations.

data is observed:

a) the personal data must be observed by reasonably expected means; and

b) the personal data must be observed at a location or event at which the individual appears and that is open to the public.

12.63 Personal data is observed by reasonably expected means if individuals ought to reasonably expect their personal data to be collected in that particular manner at that location or event. It is important to note that this test is an objective one, considering what individuals ought reasonably to expect instead of what a particular individual actually expects (which would vary from individual to individual).

> Example:
>
> Jeff is strolling down the aisles in a shopping mall. It would be reasonably expected that his image would be captured by CCTVs installed by the mall for security reasons.
>
> Jeff enters Store ABC to make a purchase. It would be reasonably expected that his image would be captured by CCTVs installed by Store ABC for security reasons. However, as good practice, Store ABC should put up relevant notices to inform its customers about the CCTVs in operation.
>
> Jeff subsequently enters Store XYZ, who has engaged a photographer for the day. Generally speaking, photo-taking is reasonably expected in a location like a store that is open to the public. Therefore, it would be reasonably expected for Jeff's personal data to be captured by Store XYZ's photographer (or by other photo-taking equipment, e.g. smart phones of fellow patrons). However, as good practice, Store XYZ should put up relevant notices to inform its customers about the photographer.
>
> Jeff leaves the shopping mall and enters a public park where filming for a TV show is taking place. His image was captured by the film crew in the course of filming the show. In this case, it would be reasonably expected that his image could be captured by the film crew. However, as good practice the film crew should put up notices at appropriate locations (e.g. at the entrances to the park) to inform park users that filming is taking place.

12.64 A location or event would be considered "open to the public" if members of the public can enter or access the location with few or no restrictions. Generally speaking, the more restrictions there are for access to a particular location, the less likely it would be considered "open to the public". Relevant considerations would be factors that affect the ease and ability with which the public can gain access to the place. Examples include the presence or absence of physical barriers, such as

fences, walls and gates, around the place; the conditions and effectiveness of these barriers; and the employment of security systems, sentries and patrols aimed at restricting entry.

12.65 However, the mere existence of some restrictions is not sufficient to prevent the location from being regarded as open to the public. For example, events that may be entered only upon payment of a fee by a member of the public may be considered to be open to the public for the purposes of the PDPA. Similarly, special events for members of a retailer's loyalty programme may also be considered open to the public, depending on relevant factors such as whether the event was open to a large number of members.

12.66 The Commission recognises that there can be private spaces within public spaces. In some situations, a private event may be held at a location that is usually open to the public. For example, an individual may book an entire restaurant for a private dinner. In such situations, as members of the public cannot enter the location during the event, the event is not open to the public. In addition, a location is not open to the public merely because members of the public may look into the premises or location. For example, if members of the public are not able to enter residential premises or commercial premises that are closed for a private event, the ability to observe what is happening inside the premises would not make the premises open to the public. Another example would be the interior of a taxi for the duration when it is hired by a passenger. During the period(s) of hire, the interior of the taxi would not be considered a location that is open to the public, even though the taxi itself may be in a public space. The "publicly available data" exception may not apply to such private spaces within public spaces and an organisation must typically provide appropriate notification and obtain consent before collecting, using or disclosing personal data (e.g. in-vehicle video cameras which collect personal data of the passengers in a taxi)[13].

12.67 For the avoidance of doubt, the PDPA provides exceptions for news organisations to collect, use and disclose personal data without consent solely for its news activity, regardless of whether the personal data is publicly available. Please refer to the PDPA for full definitions of "news organisation" and "news activity".

[13] The Commission recognises that organisations may have to collect, use or disclose personal data in private spaces within public spaces for reasonable purposes – e.g. to monitor in-vehicle activities for the safety of the taxi driver and the passenger.

Example:

Charles wishes to organise a birthday party for his son David. Charles books a private room within a fast food restaurant for the occasion and invites twenty of David's friends and their parents. The private room is right by the general dining area and the interior can be seen by other patrons through the glass windows. The fast food restaurant management puts up a sign at the entrance of the private room which says "Reserved for Private Event: David's 8th birthday party". Charles keeps the door closed at all times and keeps an eye on it to ensure that only invited guests enter. The birthday party would not be considered open to the public because members of the public (who are not invited to attend) are unlikely to be able to gain access to the event.

Mary similarly wishes to organise a birthday party for her daughter Jane. She invites twenty of Jane's friends and their parents to gather at the same fast food restaurant at a particular date and time but she does not book a private room or area within the restaurant. Her guests occupy a large area within the fast food restaurant's general dining area. Mary's birthday party would be considered open to the public even though she did not open attendance to the public, because members of the public may enter the general dining area of the restaurant and may seat themselves close to or even within the area where her party guests are seated.