Unsolicited Electronic Messages Act 2007

Prohibiting Spam and promoting good business practice

This guide provides practical information so businesses can ensure they meet the requirements of the Unsolicited Electronic Messages Act 2007.

The Department of Internal Affairs

Te Tari Taiwhenua

What is spam?

The Unsolicited Electronic Messages Act 2007 (the Act) prohibits electronic spam with a New Zealand link (i.e. messages sent to, from, or within New Zealand).

The Act refers to spam as 'unsolicited commercial electronic messages'.

'Electronic messages' encompasses emails, instant messaging, SMS, multimedia message services and other mobile phone messaging (but does not include voice or fax).

In order to be considered spam the electronic message must also be commercial in nature – for instance marketing or promoting goods, services or land, or directing the recipient to a location where a commercial transaction can take place (such as a website). It is important to note that providing a hyperlink to a company web page in the signature of an otherwise non-commercial email may make it commercial, if the web page markets or promotes goods, services, land, a business or an investment opportunity.

There are many commercial electronic messages that can be sent legitimately. They are only spam if they are sent without the consent of the recipient – as unsolicited messages.

Note: A single message may be spam. The message does not need to be sent in bulk, or received in bulk.

Spam checklist

1) Is your message electronic?
2) Is your message commercial?
3) Is your message unsolicited?

The message is only spam if it fits all three of these criteria.

Sending commercial electronic messages

In addition to prohibiting spam, the Unsolicited Electronic Messages Act 2007 lays out rules for sending commercial electronic messages. The message must contain:

- Accurate information about the sender of the message, including how they can be contacted
- A functional way for the recipients to indicate that they do not wish to receive such messages in the future – that they wish to unsubscribe.

Businesses also must not use electronic address harvesting software, or lists that have been generated using such software, for the purpose of sending unsolicited commercial electronic messages.

Which messages are not commercial electronic messages?

The Act provides that the following common messages between organisations and clients/customers are not considered commercial electronic messages:

- Responses to a request for a quote or estimate
- Messages that facilitate, complete or confirm a commercial transaction that the recipient previously agreed to
- Warranty information, product recalls and safety and security information about goods or services used or purchased by the recipient
- Factual information about a subscription, membership, account, loan or similar ongoing relationship
- Information directly related to employment or a related benefit plan in which the recipient is currently involved
- Messages delivering goods and services, including product or upgrades, that the recipient is entitled to receive under the terms of a previous transaction.

If a message falls into any of the above descriptions then it is not spam, and it doesn't have to contain information about the sender or a functioning unsubscribe facility.

Penalties

The Act specifies a number of options that are available to enforce the legislation, depending on the circumstances. The range of possible activities includes formal warnings, infringement notices and court actions.

A business that is found to be in breach of the Act may be subject to a court imposed penalty of up to $500,000. The business could also be made to pay the victims compensation up to the amount of loss suffered or damages up to the amount of profit that was made as a result of sending the spam.

What should I do?

When reviewing your business practices and the content of your electronic commercial messages to ensure you comply with the Act, there are three steps to follow.

Step 1 – Consent

Commercial messages must not be sent unless you have *express consent*, *inferred consent*, or *deemed consent.*

Express consent is a direct indication from the person you wish to contact that it is okay to send the message(s). Express consent can be gained in a variety of ways such as:

- Filling in a paper form
- Ticking a box on a website
- A phone or face-to-face conversation.

Businesses should keep a record of all instances where consent is given, including who gave the consent and how. Under the Act it is up to the sender to prove that consent exists.

It is also advisable to verify that consent has come from the actual holder of a particular electronic address. This can be done by requesting that the recipient reply to confirm they would like to receive future messages.

If you are using an existing database of addresses and you are not sure if you have the express consent of the people listed you will need to obtain it, unless one of the other forms of consent apply.

> Example 1:
> Keith runs a retail business and publishes a customer newsletter. Since he started the newsletter he has used mailing list software which only subscribes people to the mailing list if they enter in their email address on a website, and confirm by email their desire to be subscribed.
>
> ✔ Keith has *express consent* and is complying with the Act.

Inferred consent is when the person you wish to contact has not directly instructed you to send them a message, but it is still clear that there is a reasonable expectation that messages will be sent. For example, the address-holder provided their email address when purchasing goods and services in the general expectation that there will be follow-up communication. Another example is swapping business cards.

If someone has been on your existing address list and has not 'unsubscribed', it does not mean that consent can be inferred.

If you are not confident that the existing relationship is strong enough to infer consent, you should obtain express consent.

Inferred consent is limited in its application. For example if people join a tennis club you can infer consent to send them a tennis newsletter, but you could not infer consent to send them an investment newsletter.

> EXAMPLE 2:
> Natalie manages a gym and sends out a fitness newsletter to 1,500 people. Gym members were asked to provide an email address when they signed up but many of the addresses on the list are not current members.
>
> X Natalie has the *inferred consent* of her gym members but not from those people on the list who are not currently members. Natalie will be in breach of the law if she continues to send her newsletter without knowing if recipients have consented to receive it.

Deemed consent is when someone *conspicuously* publishes their *work-related* electronic address or mobile number (e.g. on a website, brochure or magazine). However if a publication includes a statement that the person does not want to receive unsolicited commercial electronic messages at that address, consent cannot be deemed.

However, the message sent must be relevant to the recipient's business.

> EXAMPLE 3:
> Joe notices a sign that publicises the email address of a car yard. He sends an electronic message to that address advertising the office furniture his company sells.
>
> X This would be considered spam as Joe's message is irrelevant to the car yard. However, if Joe's company sells goods and services related to the car industry, this would be considered *deemed consent*.

STEP 2 – IDENTIFY

Commercial electronic messages must always clearly identify the business responsible for sending the message and how they can be contacted.

Sometimes you might use another organisation, a third party, to send commercial electronic messages on your behalf. This third party must include accurate information about your business, i.e. name and contact details. The amount of information may depend on the medium by which the message is sent. Text messages impose limitations on the amount that can be displayed.

Identification details that are provided must be reasonably likely to be accurate for a period of 30 days after the message is sent. This requirement ensures that addressees have a reasonable chance of being able to contact you.

Step 3 - Unsubscribe

Commercial electronic messages must contain a functioning unsubscribe facility, allowing people to state that commercial messages should not be sent to them in the future. It needs to be clearly presented and easy to use. It could be as simple as a line in your message saying, 'If you do not wish to receive future messages, send a reply with UNSUBSCRIBE' in the subject line.

However, if you have an ongoing arrangement/contract with the recipient of your message waiving this requirement you will not need to include an unsubscribe function.

There must be no cost to the recipient for using the unsubscribe facility, and you must honour a request to unsubscribe within five working days, or else any subsequent emails will be regarded as unsolicited.

Similar to the identification of the message's sender (in step 2) the unsubscribe facility must be reasonably likely to remain accurate and functional for a 30 day period. It need not be an automated process, but should be reliable.

> Example 4:
> Judith owns 'Beautiful U' beauty salon and has express consent to send her clients promotional text messages. She includes 'Beautiful U. Reply OPT-OUT to unsubscribe' at the end of every message. The cost of the reply is reverse billed to Beautiful U.
>
> ✔ Judith has fulfilled the requirements of the Act by clearly identifying the sender of the message and how the recipient can contact them for free to unsubscribe.

The Privacy Act

In addition to the requirements of the Act, you should always comply with the Privacy Act 1993 and be familiar with the Privacy Principles.

Passing on email addresses, without permission, to another organisation or business may breach the Privacy Act.

The Privacy Commissioner's Office provides a comprehensive range of information on the requirements of the Privacy Act at: www.privacy.org.nz/privacy-act

More information

For more information about spam and the Act see www.antispam.govt.nz