

WE KNOW

# MARKETING

## UNSOLICITED ELECTRONIC MESSAGES ACT

QUICK GUIDE

The Unsolicited Electronic Messages Act – otherwise known as the Anti-Spam Act came into force in September 2007.

### WHAT IS IT AND WHO IS AFFECTED?

The Unsolicited Electronic Messages Act is designed to tackle the proliferation of unsolicited commercial electronic messages. The legislation relates to organisations **and** individuals involved with sending such messages. If you send any form of 'commercial electronic message' as defined in the Act, your activity is covered by this legislation.

It is important that you include your anti-spam measures in your ICT policy so that your staff are aware of what is required to comply with the law – especially since individuals as well as organisations can be liable for breach of the legislation. Ensure you are aware of the email practices of your employees.

### WHAT TYPE OF MESSAGE IS COVERED BY THE ACT?

Unsolicited commercial electronic messages are covered by the Act. This includes emails, TXT/SMS, instant messages, and facsimiles which market goods, services, land or business or investment opportunities. A message that provides a link, or directs a recipient to such a message is also caught. There is a list of exemptions. For example, messages that provide quotes, confirm commercial transactions or provide information directly related to an employment relationship or related benefit plan are not caught.

The 'unsolicited' bit essentially means you need to have the consent of the recipient before the commercial electronic message is sent.

There is no minimum number of messages required before the Act kicks in. Consequently a wide range of messages is captured by the legislation, from bulk mailouts to one-off emails

### HOW DO I GET CONSENT?

Consent can come in three ways:

- Express – that's when the receiver has specifically given you permission
- Inferred – arises where consent can be reasonably inferred from the conduct and the business and other relationships of the persons concerned
- Deemed – arises where the receiver's electronic address is conspicuously published in a business or official capacity (e.g. on a website) with no statement restricting the use of that information. However, your message to that address must be relevant to the business or official capacity of the receiver.

If you are unsure whether you have consent from a person on your email marketing list, it is advisable to make contact prior to issuing any communication to them. You may end up with fewer on your database as a result but those you do have left will be people who really want to hear from you.

## **WHAT SENDER INFORMATION DO I NEED TO INCLUDE?**

Commercial electronic messages need to include accurate sender information, i.e. who authorised the sending of the message and how the recipient can contact that person.

## **DOES THIS SENDER INFORMATION ALSO APPLY FOR TXT MESSAGES?**

Yes it does. This is a challenge for texting given the number of available characters to get your message out and include accurate send details.

## **HOW DO I HANDLE PEOPLE WHO WISH TO OPT OUT OF RECEIVING MESSAGES?**

It is compulsory to have a functional opt out facility on ALL commercial electronic messages. This has to be available at NO COST to the person receiving the message. Another challenge for TXT messages! This opt out must be valid for 30days from when the message is sent (another issue for some TXT systems) and you need to ensure your systems are in place to be able to action the opt out within five days.

## **ARE THERE ANY RULES ABOUT EMAIL ADDRESS & MOBILE NUMBER LISTS?**

Using address-harvesting software or harvested address lists in connection with sending unsolicited commercial electronic messages is expressly prohibited. Address-harvesting software is software which searches the internet for email addresses and collects and compiles those addresses.

## **WHAT ABOUT VIRAL MARKETING CAMPAIGNS?**

The Act does not specifically refer to viral campaigns (forwarding commercial emails on to personal contacts). Suffice to say that commercial electronic message cannot be sent without first obtaining the consent of the recipient. The law does refer to offences for aiding, abetting or inducing a breach of the Act, so be very careful.

## **DO ANY OTHER LAWS AFFECT SENDING ELECTRONIC MESSAGES?**

Short answer, yes. For example, you must comply with the Privacy Act 1993. There are 12 Privacy Principles and, in particular, principle 3 requires that you:

- Tell people when you're collecting personal information (this includes the individual's email address and mobile phone number)
- Explain what it will be used for
- Tell them who will hold it and who has access to it
- Make them aware of their rights of access to their own personal information, and request correction of such information.

This might be a good time to review your privacy statement.

## **HOW ARE COMPLAINTS ANSWERED?**

Complaints will be handled by the Department of Internal Affairs.

## **WHAT ARE THE CONSEQUENCES OF BREAKING THE LAW?**

The Act can be enforced by seeking injunctions and compensation and damages. There is a process for formal warnings and the issue of civil infringement notices. The fishhook is that you could also be liable for penalties (up to \$200,000 for individuals, and \$500,000 for organisations).

## **PROTECT YOURSELF AGAINST RECEIVING UNSOLICITED COMMERCIAL ELECTRONIC MESSAGES**

You may also want to consider taking steps to ensure you don't receive unsolicited commercial electronic messages. For example, where you have contact details on your website you might want to add a line that specifically states that the contact details should not be used for unsolicited commercial electronic messages.

## **ACTIONS**

Things to action immediately:

- Make sure you have consent from everyone on your electronic marketing database
- Identify yourself clearly in a commercial electronic message, and include a free functional unsubscribe facility (in other words, an opt out facility)
- Make sure your systems processes opt outs within five working days
- Add a 'no unsolicited commercial electronic messages' message alongside email addresses on your website for your own email addresses (if you don't want to receive such messages)
- Set up an internal contact for 'complaints' from recipients so you are proactively addressing any potential issues
- Ensure your ICT policy is up-to-date and your staff are aware of it.

## **FOR MORE INFORMATION ON THE ANTI-SPAM LAW VISIT**

Department of Internal Affairs: [www.dia.govt.nz](http://www.dia.govt.nz). For People, Communities & Businesses, Anti-Spam Complaints.

---