The marketer's guide to

Email Spam Law in New Zealand

Calibrate

Table of Contents

Calibrate

Disclaimer

This guide is not a legal opinion and must not be used as one.

Introduction

A decade has passed since New Zealand enacted the Unsolicited Electronic Messages Act 2007 (the Act) to protect kiwis from unsolicited electronic messages.

New Zealand's Department of Internal Affairs (DIA) have a team called the Electronic Messaging Compliance Unit (the Unit) that is dedicated to upholding this legislation and investigating spam complaints. After coming to the attention of the Unit, hundreds of organisations and individuals have been given formal warnings and civil infringement notices, several of which have been as far as the High Court. This costs time and money and embarrassment as every month the Unit publishes a list to their website of everyone who is caught in their net.

On page 4 you can read the Unit's summary of the Act written especially for marketers reading this guide.

New Zealand marketers want to do the right thing, and our team at Calibrate is often asked to interpret the intention of the Act and explain how it affects day to day marketing activity. We are a technology focused digital agency and our legacy in email marketing means some of our team has been involved for over a decade in the Act's inception, development, enactment and enforcement. We have worked closely with the DIA over this time and we understand their approach and intent.

Ten years on we have seen we have seen great marketers get caught out by bad technology, poor processes and bad advice. To help New Zealand marketers navigate the Act, we developed this guide to use in your business.

Every New Zealand business has a legal obligation to adhere to the Act for electronic communications sent by you, or on your behalf, to New Zealand-based email recipients. There are a set of simple requirements and, once you know them, compliance is straight-forward. But it's not easy to read the Act itself.

Unsolicited Electronic Messages Act 2007
http://www.legislation.govt.nz/act/public/2007/0007/latest/DLM405134.html

To get the most from this guide:

- Read it cover to cover.
- Distribute to marketing and communications roles.
- Refer back to it when inducting new staff.
- Tick off the Compliance Checklist.
- If in doubt seek legal advice.

What is Spam?

The Act defines *spam* as 'unsolicited commercial electronic messages' and it covers emails, fax, instant messaging, mobile/smart phone texts and image-based 'text' messages of a commercial nature. It does NOT cover Internet pop-ups or voice telemarketing.

This handy guide goes into the details of how the government defines spam and, if you follow it, you are unlikely to get into any trouble. But we all know that it is the customer who is always right.

Consumers regard spam as anything they don't want to get. Never mind if they signed up for it – they have the power to judge how relevant and valuable your information is to them, and no means no. People will use the JUNK button, the unsubscribe link, or email you to tell you to stop. That's a good thing! For example, if they were house-hunting, they couldn't wait to get your weekly new listings guide but, once they have signed the mortgage, they will probably want your email gone forever. Keep that in mind when reviewing your unsubscribe rates. People change and, when they want to move on, you need to bow out gracefully and keep on being relevant and valuable to everyone else.

“

Comment from the Regulator

Complying with the Unsolicited Electronic Messages Act 2007 is not difficult if the right business practices are implemented before an entity sends a commercial electronic message (i.e. email, SMS, fax, instant). The Electronic Messaging Compliance Unit at the Department of Internal Affairs (the Unit) has recently introduced a new reporting webform (www.reportspam.co.nz) for recipients who wish to complain about commercial electronic messages that they have received. Already, the Unit has noticed a sizeable increase in the number of complaints received per month.

To ensure that your entity is not the subject of one of these complaints, there are a number of basic steps you, as a sender, can take to mitigate the risk of a complaint being made:

Ensure that you can demonstrate consent for each recipient of your commercial electronic messages.

- The best form of consent that a sender can rely on is express consent, where a person actively opts in to receive messages from you. The Unit recommends building a database where you can demonstrate express consent for each recipient's electronic address(es).

- If you are intending on relying on inferred consent, ensure that you can demonstrate the existence of an ongoing business relationship between you and the recipient.

- Often, complaints are made to the Unit because the sender believes that they can rely on deemed consent. However, when the Unit investigates a complaint and the sender is relying on deemed consent, it is a regular occurrence that the sender will not be able to prove that the message is relevant to the recipient in their business or official capacity. Since the sender cannot demonstrate deemed consent in these instances, the Unit may elect to take enforcement action for the identified breach of the Act.

Ensure that you include accurate details in your message relating to who the sender of the message is.

Ensure that your message includes a functional unsubscribe facility.

- Ensure that, if a recipient chooses to unsubscribe from receiving further commercial electronic messages from you, the recipient is removed from your commercial electronic messaging database. This includes direct requests made to you, outside of the unsubscribe facility, to remove a recipient's electronic address.

- The Unit regularly sees complaints submitted after the recipient has made repeated requests to unsubscribe from receiving further commercial electronic messages from that sender. If you receive an unsubscribe request, remove that recipient's electronic address within 5 working days after the unsubscribe request was made. Failing to include an unsubscribe facility, or honouring an unsubscribe request within the allocated timeframe, will constitute a breach of the Act for which the Unit may take enforcement action.

The Unit also recommends ensuring that there is a managed interaction with third-party providers of electronic messaging services. Issues often arise when a sender relies too heavily on technology without appropriate oversight of how the technology is being used by recipients, specifically with regard to the functionality of the unsubscribe facility.

The Unit takes compliance with the Act seriously. The Unit may investigate any complaint that is lodged and may elect to take enforcement action if a breach of the Act is identified as a result of that investigation. Enforcement action the Unit may take ranges from issuing a formal warning to issuing a civil infringement notice, including a financial penalty of up to $200,000 for individuals and $500,000 for organisations. Therefore, it is important that you take your compliance obligations with the Act just as seriously as we do and implement the appropriate processes and procedures to ensure that your commercial electronic messages comply with the regulations outlined in the Act.

The Unit is always approachable for any questions, queries or concerns you may have regarding compliance with the Act. We encourage you to contact us if needed and are happy to talk with you over the phone, through email, or in person. You can find our contact details at **www.antispam.govt.nz**

Kind regards,
The Electronic Messaging Compliance Unit
Department of Internal Affairs, Government of New Zealand

The Marketer's Guide to the Spam Act

Five Steps to Email Compliance

1. Have consent* to send commercial electronic messages
2. Quickly and permanently action unsubscribe requests.
3. Identify yourself accurately.
4. Don't use harvested data lists.
5. Put good record keeping and processes in place so you can prove* that you do all of the above.

* *The UEM Act 2007 is a Civil, not Criminal, Act so when you're contacted by the DIA with a "please explain", the onus is on you to prove that you are NOT in breach rather than on them to prove you are. If you don't have good records to help you out, then, at worst, you stand to be prosecuted and, at best, you will waste a lot of time finding proof in retrospect.*

Step 1 - Have Consent

The Act says that you need permission from your prospective recipient before you can send a commercial electronic message. **Under the Act, there are three types of acceptable consent—express, inferred and deemed.** You can obtain consent by direct request or, to some extent, it can be assumed by the nature of your business and its relevance to the recipient.

We find that it helps if you think of the three acceptable levels of consent as a set of traffic lights when it comes to how readily you can use them:

Express: Green

go without a second thought.

Inferred: Orange

proceed but look around for reasons why you might need to stop.

Deemed: Red

stop, look and think hard before you proceed.

To prove consent, make sure that the source is recorded when you collect it.

Express Consent

What it's about

These people have willingly and specifically requested or consented to receiving the communication that you are sending.

What you need to do to comply

Ask for permission and record this consent permanently on your database. Verbal consent is okay. There is no obligation in the UEM Act 2007 for the consent to be in writing, but it is always a good idea to keep a written record of verbal consent.

Our recommendation

To have express consent, you will have asked them to register for the specific message type. This is also known as opt-in, sign-up, permission, registration etc. Allowing your recipients to alter their permission in a **preference centre** is a best practice, which means that they can easily choose which of your publications they receive and how regularly they receive them.

Inferred Consent

What it's about

Inferred consent means that you don't have express consent but you can infer permission if you are sending relevant business information such as customer service notifications, invoices, reminders, or sending an invitation to reconnect with a lapsed customer.

What you need to do to comply

Ensure that you have a prior, relevant business relationship with the people you are sending emails to and keep a record of this in your database. Also, apply common sense and a customer view of the length of time a relationship remains valid.

Our recommendation

Do not email if it's unlikely that they will easily remember the relationship you had. For example, if they stayed at your hotel three years ago, don't start emailing them now. But if they buy a car from you every three years, then you could email them to check if they are ready for another

Deemed Consent

What it's about

Your publication must be relevant to the business. You may send it to an electronic address that has been published by a person in a business or official capacity (e.g. on a company website).

What you need to do to comply

Record where you sourced the email address from (e.g. website) and ensure relevance. For example, if you sell downpipes, you can email plumbers. If you sell cat doors, you can't.

Our recommendation

This is getting into red-light territory. Copy and tone will help ensure that your email doesn't cause anyone to get their back up.

Tip

To protect your own team against being 'harvested' from your website, put a statement on there saying that you deny permission to use any published email addresses for the purpose of sending marketing email.

Step 2 - The Unsubscribe Process

All email and SMS messages must contain accurate contact information for the organisation and provide a working unsubscribe method. You must quickly and permanently action unsubscribe requests.

What it's about

- Your unsubscribe method must be obvious and working
- It needs to be actioned within five working days
- Failure to do so may result in a fine of $10,000

What you need to do to comply

Never send commercial messages without allowing the recipient to unsubscribe. Use email software that automatically and permanently unsubscribes. Actively manage response email addresses in case someone chooses to email their unsubscribe request rather than use the link on your email.

Our recommendation

People can unsubscribe by replying to your email, ringing you up or messaging you on social media. You have to action all of these, so you need a system for doing so. It's not uncommon for a recipient to email you from one email address complaining that you did not action their unsubscribe request.

Tip

Ensuring the email carries a merge field which indicates the email address that you are holding for this recipient (e.g. "you are subscribed as #email#) will give a good protection from misunderstandings about which email address has been used for this publication. Many people have more than one and get confused about which they subscribe and unsubscribe with, making tracing the audit trail more difficult, time consuming and expensive. This applies to all emails, including stakeholder communications, news releases and customer service email notices such as "here is your record of travel for this month". You can link to an update area so that they can change the details if they're wrong.

Step 3 - Harvested Data

What it's about

Don't use harvested data, which is a list made by software that rolls through the internet ripping off addresses from websites, blogs, etc.

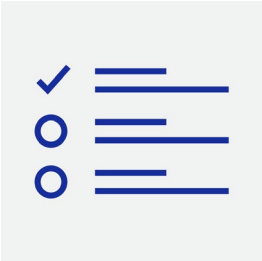
What you need to do to comply

Check the source of the data you are using.

Our recommendation

This one is not really relevant to marketers as it applies to actual spammers.

Step 4 - Sender Details



The sender and the subject line must not be misleading. You should make it easy for the recipient to contact you by having contact details in the email or a working link to your website contact page.

What it's about

All messages must have a clear and accurate "from", "subject line" and contain the senders contact details.

What you need to do to comply

Any electronic message must clearly and accurately identify the person who authorised the sending of the message and must include accurate information about how to readily contact that person.

Our recommendation

In the USA's CAN-SPAM law, it's a requirement to show a street address. That isn't strictly necessary in New Zealand, but it does add credibility and a sense of bricks and mortar to your brand—especially for ecommerce.

Step 5 - Record Keeping

Put good record keeping and processes in place so you can prove that you are compliant.

Your team needs to know that there is a legal obligation to abide by the provisions of the UEM Act 2007 and also know the consequences of not adhering to them. Your company needs to have adequate and compliant email practices and technology in place. In best practice, an actual person is responsible for the electronic messages sent, is clearly identified within your organisation and is equipped to comply as required.\

You must to be able to show consent, non-harvested data and proof of your good process and intention. So, you could implement some or all of the following to show that:

You have consent

The onus is on the sender and the sender organisation to prove their description of process or events. Record when, where and how the recipient opted-in to your database. If it's possible the recipient may not be 100% sure of the relationship, use copy in the email that is polite and explains the purpose of the email.

Remember the law of brand elasticity? The more people like you, the more they will forgive genuine mistakes, and the less likely they are to complain.

Use your manners and be likeable!

Tip

Your intent is important. If you can show that you did not intend to offend or breach the Act and that you had steps in place to make sure this didn't happen, then you may still be warned or sanctioned but you are unlikely to be prosecuted.

You are not using harvested lists

Don't use harvested lists and be prepared to show where, when, and how the recipient is on your database.

You made a 'mistake' or had an 'accident'

The UEM Act 2007 allows the defence "that person sent the message, or caused the message to be sent, by mistake". Using a sending checklist and retaining copies of each of these will provide the evidence that you'll need of the error if one occurs. Be prepared to show what systems and processes you have in place to ensure that your messages are compliant. Be upfront about mistakes and put steps in place to prevent them happening again—record these actions in case you forget what you did and why.

?

What's Exempt from the Act?

Emails sent by the government are exempt and so are things that relate to delivery of goods or services, like warranties and contracts. There are quite a few areas, so we've included Section 6, Part B of the Act below, which outlines what the Act does not cover.

……..

Exemptions include an electronic message that:

(i) provides a quote or estimate for the supply of goods or services if that quote or estimate was requested by the recipient; or

(ii) facilitates, completes, or confirms a commercial transaction that the recipient previously agreed to enter into with the person who authorised the sending of the message; or

(iii) provides warranty information, product recall information, or safety or security information about goods or services used or purchased by the recipient; or

(iv) provides notification of factual information about a subscription, membership, account, loan, or similar relationship involving the ongoing purchase or use by the recipient of goods or services offered by the person who authorised the sending of the message, or the recipient's ongoing subscription, membership, account, loan, or similar relationship; or

(v) provides information directly related to an employment relationship or related benefit plan in which the recipient is currently involved, participating, or enrolled; or

(vi) delivers goods or services, including product updates or upgrades, that the recipient is entitled to receive under the terms of a transaction that the recipient has previously entered into with the person who authorised the sending of the message; or

(vii) provides the recipient with information about goods or services offered or supplied by (A) a government body, or (B) a court or tribunal; or

(viii) has any other purpose set out in the regulations.

The Marketers Spam Law Compliance Checklist

Page 1 of 2

Action	Justification	Tick
Your whole team is aware of the UEM Act 2007 and its implications to them and your business.	The company or person authorising the sending of electronic messages should know they have a legal obligation to comply.	☐
You are confident that every place you collect information from your clients and prospective clients states your intention for the use of the data and, if your intentions change, you have a process to inform them.	Ask for consent in everyday language and rely on opt-in, not opt-out. Usually, we recommend that you don't pre-tick permission boxes unless the reason they are signing up is a part of the call to action.	☐
Your CRM system stores the source of email marketing consent.	Record source and date – For example in-store or homepage, campaign name, shopping cart, call centre, registration form, trade fair, phone enquiry, etc. Collect the date stamp if it's an online opt-in.	☐
You have a process to regularly review all of your email marketing deployments. What are you sending, when, to who?	Review your emails including stakeholder communications, lifecycle marketing, sales emails and everyday transactional customer service notices. What are you sending via email? Who's it going to? What does it look like? What business goals does it meet? Is it best practice? How can you improve it?	☐
Your marketing communications team uses a deployment checklist every time an email is sent.	Email **campaigns@calibrate.co.nz** to get a copy of a generic deployment checklist to keep these records.	☐

continued next page

The Marketers Spam Law Compliance Checklist

Page 2 of 2

Action	Justification	Tick
You actively manage your email marketing systems. This includes API and other middleware that can also stop working and prevent normal data and systems function.	The Unit expressly recommends that you make sure you have managed interaction with third-party providers of electronic messaging services. Issues often arise when a sender relies too heavily on technology, without appropriate oversight of how the technology is being used by recipients.	☐
You have a good process for unsubscribe requests.	Make sure that your unsubscribe link is working and check it regularly. Make sure it is actioned within 5 days and that every email has an active unsubscribe link for 30 days after it's been sent. Have processes to monitor reply email inboxes, call centres, etc., so that you action manual unsubscribe requests.	☐
Review all email templates for best practice features. Make recommended insertions standard in all templates by default.	Insert email address of the recipient into each email so you can find it in your database (e.g. "you are subscribed as #email#). Insert full contact details of your company and the name of the person who authorised the email send.	☐
Review the reputation of your business as an email sender and instigate best practices. Consider DomainKeys, SPF, DNS Registration, and isolated rather than shared IP Addresses.	It's a good idea to review your platform setup as it is likely to deliver better inbox placement if you go further than the basic configuration provided by your email software vendor. Assigning a subdomain for commercial and transactional emails and registering for industry recognised identification is a best practice.	☐

If your team would like a little or a lot of help in taking your email marketing to the next level, our **Calibrate** experts are here at team@calibrate.co.nz and +64 9 600 1478. If you have concerns about The Unsolicited Electronic Messages Act 2007, we recommend that you seek advice from your legal team.

References and Resources

The complete Unsolicited Electronic Messages Act 2007
www.legislation.govt.nz/act/public/2007/0007/latest/DLM405134.html

The Marketing Association is the industry body for marketing in New Zealand, offering specialist regulatory and legislative resources and advice.
www.marketing.org.nz

The Department of Internal Affairs Anti-spam compliance team FAQ page
www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Anti-Spam-Questions-and-Answers?OpenDocument

List of the companies who have been prosecuted in New Zealand
www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Anti-Spam-Enforcement-Action

A summary of New Zealand spam statistics
www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Anti-Spam-Results-and-Statistics

Global Spam Guide
Do you operate in more than one country? You are able to buy this quick look-up matrix of countries by email compliance requirements. It currently covers over 75 jurisdictions.
emailexperience.org/email-resources/eec-global-email-marketing-compliance-guide/#!form/GlobalComplianceGuide

Calibrate

Created by Calibrate Marketing Limited.
May be reproduced with credits intact.

Lets work together

09 600 1478