Code of Conduct for Marketing to Organisations by E-mail

Contents

This document was last updated in April 2013.

Introduction

SWEDMA's objectives for these guidelines are to:

- encourage the positive development of e-mail as an effective marketing device
- increase awareness of the ethical and legal matters that clients need to be conscious of when using e-mails for marketing purposes
- share examples and practice showing how clients can maximise their use of this means
- contribute to increasing quality in this sector and to discourage the increased incidence of undesired mass mailings (i.e. junk mail or spam).
- provide practical advice on the implementation of working methods and fulfilling standards for the internet.

These guidelines are chiefly concerned with marketing by normal e-mail, and not with marketing to mobile telephones via SMS or MMS. The guidelines have been compiled by Sweden's leading representatives of e-mail marketing, who have shared their knowledge to create a framework and guidelines for effective, ethically acceptable marketing by e-mail.

These guidelines summarise the most important points about e-mail marketing to individuals, and act as a complement to other relevant Codes of Conduct, such as SWEDMA's ”General Code of Conduct for Direct Marketing by Mail” and the International Chamber of Commerce's (ICC) ”Advertising and Marketing Communication Practice Consolidated ICC Code”. SWEDMA's guidelines are not a replacement for relevant legislation, as for example the Personal Data Act (Personuppgiftslagen - PuL) and the Marketing Act (Marknadsföringslagen - MFL), details of which appear in the appendix. Additionally, contracts with internet service providers (ISP) and their guidelines for acceptable use of their networks must also be observed.

It is easier for you, the readers of these guidelines, to understand and take them on board if you start with the vocabulary at the end of this document, under item 8.

These guidelines are aimed at all who engage in sending e-mails to businesses. Please note that the rules for e-mail communications to organisations are different from those to private individuals, and that it is permissible to send relevant information or advertising by e-mail to persons connected to businesses that are not customers. It is essential always to operate with an updated address database and the message should be relevant to the recipients in their professional capacity. We list a number of items below which you need to be aware of, and which laws and recommendations we consider to be applicable.

1. COMMUNICATION OF RELEVANCE TO THE RECIPIENT

E-mails sent to addresses that are clearly connected to an organisation, e.g. info@company.se, are always deemed to be directed to a business.

E-mail marketing to companies also covers individuals who are contacted in their professional capacity. In these cases you do not need to have the active agreement of the company or individual, as long as the commercial communication is relevant to the recipient's professional role. The relevance must be obvious - you can send e-mails about the development of a new CRM system to a customer relations manager, but not advertising about cleaning products to that same person.

Please note that the Marketing Law (MFL) does not permit you to send e-mails addressed to persons in their private capacity, unless they have given their consent in advance.

2. OPT-OUTS

The Marketing Law requires that all e-mails must offer the recipients the opportunity to refuse further e-mails from the sender. The refusal is also known as an opt-out, which is normally done through an opt-out link that is clearly evident in the e-mail. The link should be a URL link that goes to an opt-out site.

3. SOURCE OF RECIPIENTS' ADDRESSES

If there is no established customer relationship and you send e-mails to companies or persons in their professional capacities the Marketing Law requires that you provide the source of the recipients' addresses. The address source must contain the name of the organisation from which the addresses were sourced, their address or telephone number to ensure that the recipients may easily contact the source.

4. DATA COLLECTION

4.1 Collection

Organisations that collect e-mail addresses to sell them to third parties or for use in their own business activities must consider the limitations imposed by legislation, the Personal Data Act (PuL) and the Marketing Act (MFL). It is also necessary to ensure that:

- the database is regularly updated
- the purpose of collecting the data is made clear at the time of collection
- no more data must be collected than is necessary
- there is a personal data controller, as e-mail addresses are regarded as personal data
- there are routines for removing the data of those who have notified the address source that they wish to be removed from the database, i.e. an internal e-mail preference list
- advertisers input e-mail information on an internal e-mail preference list instead of deleting the data when an opt-out request is received, so that the request is registered, kept and respected until the person concerned re-registers, which cancels the previous request for opting out
- it is possible afterwards to check when and how personal data has been collected, e.g. by noting on the register when the data was entered and the source of the data
- clear information is provided about the company's guidelines for data security and integrity (see below) and either a link to, or complete information about the guidelines that applied at the time the data was collected.

It is permissible to collect e-mail addresses of businesses from websites, e-mails and other public sources, as long as any e-mails sent out are relevant to the recipients' professional roles.

4.2 Guidelines for data security and integrity

When e-mails are collected (on or off line), information about the company's guidelines for data security and integrity must be shown prominently (or at least pointed out).

When guidelines for data security and integrity are formulated the following items must be considered:

- The guidelines must clearly identify the advertiser and provide the full company name and postal address. If it is not obvious from elsewhere on the website the guidelines should also contain information about:
    - the company's country of registration
    - the company's VAT registration number
    - membership (if any) of a trade or professional association
- The guidelines must clearly and visibly indicate the purposes for which e-mail addresses (or any other personal data) will be used, for example that it is intended to send marketing material about the organisation's other goods and services.
- The guidelines must also indicate if the personal data requested is necessary for the transaction between the person and advertiser, or whether they are optional, and the consequences of not providing the data requested
- The guidelines must state how to request deletion from the circulation lists

All policies must be easy to understand and reflect the organisation's intentions for future use of the data collected.

Regardless of whether the data is captured on or off line a link to, or information about, the guidelines for data security and integrity must always be provided when the data is collected.

4.3 Use of own data

Advertisers must, before sending any e-mails, compare their e-mail lists with their internal preference list and remove the opted-out addresses.

4.4 Use of data collected by third parties

Owners of addresses can hire out e-mail address lists in various ways.

One is to give advertisers access to the addresses to send out commercial e-mails to the business related addresses on the list under their own names.

Another is for advertisers to use host mailing. This is when an address owner or a data processor sends e-mail communications marketing advertisers' goods and services to their own e-mail database.

Regardless of which model advertisers choose to use it may be appropriate for them to check the circumstances under which the address owner captured the e-mail addresses. It is wise to have a written contract between advertisers and address owners.

Before any collaboration advertisers should check with the address owners:

- How and when the list was created
- What guidelines for data security and integrity existed at the time of the data collection
- How requests for opt-outs are handled and processed
- The list does not contain private e-mail addresses.

Advertisers should not use the address owner's data if the address owner cannot provide this information and provide suitable verification, contractual guarantees and indemnities. marketer

Advertisers using data from third parties should ensure that they store the date of inputting the data and the source from which the data was collected.

5. DATABASE QUALITY

Good procedures and maintenance of databases containing customer and prospective customer data is of importance for the recipients' trust; they also make it easier to convey messages.

Advertisers should formulate guidelines to ensure the quality of their databases; the guidelines should describe how to deal with replies, requests for opt-outs, returns and provide timelines for the removal of recipients, removal of known invalid addresses and for the verification of address formats.

The objectives of an organisation's guidelines for databases should be to:

- reduce incorrect, incomplete or out of date addresses to the greatest extent possible
- deal with opt-outs directly over the internet
- deal with opt-outs received offline within a maximum of ten working days, but at least so rapidly as to avoid the advertiser sending more marketing e-mails to those who have requested opt-outs
- inform those who have requested opt-outs from the mailing list that their request has been received

Advertisers must ensure there are systems that support this policy.

5.1 Adding data

Adding data is to link further information to a database list; this is permitted. In terms of e-mail marketing it may involve among others the following situations:

- Linking demographic data or company information to an e-mail database.
- Linking an e-mail address to an existing entry with the customer's name and address.

6. USING ADDRESSES AND DATA (IN MAILINGS)

It is important for the advertiser to go through the database to be used before each mailing to check that it has been updated and all the changes entered since the previous mailing, i.e. any address changes and opt-outs from those who do not want any more mailings.

This should be done regardless of whether the mailing is undertaken with your own database or one that has been hired. If the advertiser has hired a database, it must be check before each mailing and the company hiring the database out must guarantee the updating.

6.1 Using e-mail distributors to deliver e-mails

Address owners may, as part of their host mailing services, offer mailing solutions with an e-mail distributor (EMD).

In some cases it may be better for advertisers to let another EMD take responsibility for transmitting or distributing the e-mails. The reason may be that the duplication will enable the advertiser to follow the campaign through their own EMD as they know their reporting routines, or simply that they want to have full control of the time aspects.

Good practice permits the delivery of e-mails through another EMD, as long as certain criteria are fulfilled:

1. There is a contract between the advertiser and the address owner that describes what may and what may not be done with the data.
2. The EMD must be able to transfer opt-outs from the campaign to the address owner within 48 hours. This is essential for the quality of the database.

6.2 E-mails to sole traders

E-mail dissemination to sole traders may only be undertaken if the business/person has actively consented to it (this is also known as an "opt-in"). Consent is considered to have been given if the business has itself:

- registered its address, for example to receive newsletter, or provided the information at a trade fair, exhibition or similar
- provided its address when asked, e.g. during a survey or telephone interview
- marketed its address as a means of contact, e.g. in advertisements.

7. INTERNATIONAL ISSUES

7.1 Transferring data outside the EEA

The data integrity guidelines governing the collection of personal data must also include consent to transfer the data abroad, if there is any likelihood that the data collected will be transmitted for any kind of processing outside the European Economic Area (EEA = the 27 European Union member states, plus Iceland, Liechtenstein and Norway).

Since all such transfers are banned under the PuL (Personal Data Act), unless certain requirements are met, it is considered good practice to ask for legal advice from SWEDMA or another legal advisor when considering transferring data.

Below are some examples of how the restrictions operate.

Individual prior consent must be obtained unless there are lawful grounds for the data transfer, e.g.:

- The European Commission believes that the country of transfer has an "adequate" level of data protection. A list of the countries considered to fulfil that criterion may be found at: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm
- The transfer is carried out through a Safe Harbor arrangement, based on the US model, in which individual organisations register for work under a self-regulating system based on EU guidelines. The US Safe Harbor Scheme does not at present cover all sectors; US financial organisations, for example, may not join.
- Transfers are necessary because of a contract between an individual and an advertiser, or to implement preparatory measures undertaken in response to a request from an individual.

- There is a written and signed contract between the advertiser and the recipient of data which ensures an adequate level of data protection. There are recommended standard terms which are suitable for this purpose. SWEDMA or an other legal advisor can assist with this.

It should be noted that physical data security is considered to be a requirement for safe transfer of data. Advertisers are, for example, responsible for ensuring that regardless of where data is transferred, adequate technical and organisational measures are undertaken to safeguard data from physical theft or from hackers. Advertisers are always responsible for the measures undertaken by any data processors employed, and for ensuring that adequate legal arrangements, including data processing contracts, are in place.

7.2 E-mails received outside Sweden

Do not forget that e-mails may be received outside Sweden, and that the laws and regulations for the content and distribution of commercial e-mails in the country of reception may differ from those in Sweden. For example, in the US there is no need for active agreement to send marketing e-mails to individuals.

The EU Directive on Integrity and Electronic Communications (which has been transposed in Sweden through MFL) contains regulations governing how private individuals provide prior agreement before unsolicited commercial e-mails are sent.

EU member states are given some latitude in transposing the Directive's provisions in terms of whether they wish to extend the protection offered to persons. The outcome of these linguistic modifications and varying practices in the member states means there are small, although quite important differences in the approach to transposing the Directive into national legislation.

There are problems internationally, as some state law courts in the US have applied local laws on commercial e-mails received from other states in the US. They may adopt the same view of e-mails from Swedish advertisers.

In these cases it is wise to ask for guidance from SWEDMA, FEDMA, any other legal advisors or from the Swedish Data Inspection Board, as every country may have varying regulations.

8. VOCABULARY

Term	*Definition*
Advertiser	An organisation using their own data, or data from other sources for marketing purposes
Address owner	An organisation responsible for collecting, storing and maintaining e-mail data
E-letter	An individual e-mail message
EMD E-mail distributor	
ISP Internet Service Provider	
Customer	A person subject to personal data
Personal data	Information through which a person can be identified, either from the data alone or in combination with other data which is held, or will likely be held, by a data controller
Data controller	A person or organisation which alone or collectively determines the purpose for which, and the ways in which, personal data may or should be treated (including list brokers/handlers)
Data processor	A person who collects, stores or handles personal data for an address owner or for a data controller

Please contact us if you have any questions or observations about this Code of Conduct

Ett medlemskap
som ger effekt

P.O. Box 22500, 104 22 Stockholm
08 53 48 02 60 | direkt@swedma.se | swedma.se