

Tripolis Anti-spam guidelines

Connect. Get ready. We deliver.

1 What is spam?

Spam is unsolicited bulk e-mail and unrequested commercial, idealistic or charity related e-mail sent to recipients who did not make it clear and verifiable in advance that they granted permission for that information to be sent to them by e-mail by that specific sender. That information also includes advertisements, notices, questionnaires, brochures, and information praising the merits of certain web-site addresses, sales information and auctions.

2 The Dutch legal framework

2.1 Important information for senders, from the website of the Dutch Watchdog charged with supervising the telephone and telecoms industry (information in Dutch):
<https://www.spamklacht.nl/ik-verzend-elektronische-berichten/>

The spam prohibition in the Netherlands protects everyone. It therefore does not matter if someone receives an

unsolicited electronic message and that recipient is a private individual or a business or commercial enterprise. Both kinds of unsolicited sending of messages are equally prohibited.

Sending e-mail messages

If you send messages without having been granted permission from the recipients you may be in infringement. An individual message sent is not a problem. The spam prohibition is intended to prevent e-mails being sent out which cause unnecessary burdens on recipients. The Netherlands Telecommunications Act refers to the following parties as senders:

- The sender which in fact sends the message (the person who presses the send button);
- The sender which or who is the de facto sender (the party granting the assignment to send the messages in question).



Tripolis Solutions

We deliver

For both these parties the rules of the Netherlands Telecommunications Act apply and hence sending spam is prohibited.

Suppliers of address databases

A supplier of e-mail addresses or Telephone numbers may infringe the privacy laws of the Netherlands in certain cases. The Dutch Board of Personal Data Protection supervises this. It is also possible for a supplier of such addresses to be designated as an accomplice to prohibited spamming activities by the Dutch Watchdog and be fined for this by that body. Each infringement will render the OPTA able to review which parties should be deemed the perpetrator of the infringement.

The demands imposed by the law of the Netherlands on sending electronic messages

When you send messages, you are required to comply with the following demands:

- The recipient had to have granted you permission;
- The recipient has to be able to see from whom the messages came;
- The recipient has to be able to see how and with whom he or she may unsubscribe if he or she no longer wishes to receive these messages.

1a Prior explicit permission has to be requested

Before you may send messages the recipient has to have 'explicitly' granted you permission to do so having been 'informed'. Explicit means for example that a recipient has ticked a checkbox of him or herself on a (web) form or has completed such a form with a 'yes'. A stipulation of the General Terms and Conditions is hence not 'explicit'. Even vague descriptions like 'you give permission to receive e-mails from this company and its partners' are not 'explicit'. It has to be clear what the recipient is giving permission for precisely and you will always have to be able to prove that you received advance permission from the recipient. Work out for yourself how you would wish any potential recipient to complete any explicit granting of permission you need.

1b The use of address databases

You may only use address databases when you, the sender, has/have been granted prior permission to send electronic messages to those addresses (or telephone numbers). If you have no existing customer relationship or you are unable to show that you have been granted explicit permission to send messages to those addresses, you may not make use of address databases.

You should gather proper information about the risks of using an address database which comes from another party. Such use is often illegal.

2 A reference has to clearly identify the sender

As a sender you have to reveal your real identity in each message you send. The use of an alias or pseudonym is not allowed.

3 An opportunity has to be offered to de-register

Each message sent is required to include the possibility of de-registering - even if the recipient previously granted permission. You must permit recipients to de-register without charge and make it easy for them to do so. An extensive questionnaire which needs to be completed prior to de-registering is not any easy way to unsubscribe.

2.2 Extract from the Netherlands Telecommunications Act, on the website of OPTA the Dutch Watchdog charged with supervising the telephone and telecommunications industry.

The Netherlands Telecommunications Act – the text of the Act

The spam prohibition is laid down in Article 11.7, first sub-section up to and including the fourth sub-section of the Netherlands Telecommunications Act. The text of that piece of legislation reads as follows:

Article 11.7

1 The use of an automatic messaging system without human intervention, fax machines and electronic messages to transmit unsolicited communications for commercial, idealistic or charity related purposes to subscribers is solely permitted if the sender is able to show that the subscriber in question has granted the sender prior permission, without prejudice to that determined in the second and the third sub-sections.

2 If the subscriber, referred to in the first sub-section is a legal entity or a natural person or a natural person acting professionally or as a company, the transmission of electronic messages which have not been requested for commercial, idealistic or charity related purposes requires prior permission having been granted:

a If the sender makes use of electronic contact data when transmitting communications which electronic contact data have been designated for this purpose by the subscriber and made known, and these are used in accordance with the purposes which the subscriber attached to any use to be made of that contact data, or

b If the subscriber is established outside the European Economic Area and the regulations which apply in the country in question have been complied with concerning sending unsolicited communications.

3 Any party who has obtained electronic contact data for electronic messages as part of the sales of its products or services may use that data to transmit communications for commercial, idealistic or charity related purposes providing that the contact data was obtained at the time at which the customer was fully aware of similar products or services being offered in this manner and the customer was explicitly given an opportunity to readily, easily and without charge state no interest in receiving any such communications electronically and if the customer made no use of such an opportunity the customer is able with each and every electronic communication received to de-register and hence revoke the original permission granted in a manner which resembles those same conditions which applied. Article 41, second sub-section the Netherlands Personal Data Protection Act is accordingly applicable.

4 When using electronic messages for the purposes referred to in the first sub-section, the following information is always to be included:

- a The real identity of the party on behalf of whom or which the communication is made or sent; and
- b A valid postal address or number which the recipient may use to request termination of any such communications.

2.3 For more information

The compliance policy pursued by the Telecommunications Watchdog of the Netherlands may be referred to visiting (information in Dutch): <http://www.opta.nl/nl/actueel/alle-publicaties/publicatie/?id=2529>

FAQs may be seen by visiting (information in Dutch): <https://www.spamklacht.nl/ik-verzend-elektronische-berichten/veelgestelde-vragen/>

3 Permission

The legal requirement of permission needing to be granted in an informed manner means that in practice an opt-in needs to be arranged once it has been made clear:

- Who the sender of the mailings is;
- What the content (nature) of the mailings is; and
- How often the mailings will be sent.

Aside from this, the opt-in has to be properly recorded and registered. The onus of proof in connection with the opt-in rests with the sender. The information recorded may for example consist of: web form url, date on which that form was completed, IP of the visitor, sending time of confirmation e-mail (clicks), IP of the recipient.

Double opt-in

Tripolis advises its senders to verify any permission

granted by having the future recipient of e-mails confirm this. This is called a double opt-in. As a method, the person registering his or her interest in a service, receiving a newsletter for example is required after having registered to review a neutral confirmation e-mail in which recipients are asked to confirm their registration by clicking on a link. The use of this method means that people cannot be registered by others and those who do register really do use the e-mail address in question and that the recipient is expecting your e-mail.

4 Seven anti-spam guidelines applied by Tripolis for senders

Tripolis platforms may never be used to send unsolicited e-mails. To make it clear to users what is allowed and what is not allowed when using Tripolis systems, the following anti-spam guidelines have been drawn up. There are seven rules which users of Tripolis systems must ALWAYS obey.

1 Tripolis users may only send e-mailings to recipients who, in advance have given explicit permission to you to send them your e-mail message

This is the rule which the law imposed to be able to send recipients e-mails. You therefore have to have advance permission from recipients in order to e-mail them and you also need to be able to prove you have been granted that approval or permission.

2 Sending unsolicited commercial bulk e-mail via Tripolis is explicitly prohibited

Your actions conflict with law. Aside from this your actions have a negative influence on the reputation of Tripolis. There are recipients who deem unsolicited e-mails as spam and register their complaints with the various authorities and anti-span organizations; this may result delivery problems with other users of Tripolis.

3 It is permissible to use Tripolis to send unsolicited e-mails to customers/donors/members or other legal entities with which your organization has a customer relationship but only if those e-mails contains information about related products or services

This is the only exception to the main rule. The Netherlands Telecommunications Act gives every company and organization the right to send its own customers/members/donors/subscribers etc. unsolicited e-mails (without those recipients having explicitly granted permission to do so). The law does however require the e-mails sent being about similar products or services. The condition is also imposed that the recipient may readily unsubscribe and hence not receive future e-mail messages.

4 Tripolis users may only import opt-in files into Tripolis. When this file comes from a third party, it will have to be carefully checked to ensure that the permission needed has been granted

When you use a mailing list, you are deemed to have been convinced already that recipients of your mailing have requested receipt of your information, or have granted explicit permission to you to send them this information. You remain responsible!

5 Work using 'active prior permission'

Tripolis users are to use 'prior permission'. This means that a subscriber has to grant explicit, well informed permission to you to send him or her certain messages. Explicit means that the subscriber him or herself placed a cross on a web form or completed such a web form with a 'yes'. Setting a checkbox to a standard 'yes' is not permitted. Moreover, a subscriber also has to know what he or she is saying yes to. The recipient has to be clearly informed about what his or her e-mail address is going to be used for.

6 Each e-mail sent via Tripolis has to contain an automatic de-register or unsubscribe link

With this, the recipient can indicate that he or she no longer wishes to receive any more e-mail and do so at any time. No conditions may be imposed on de-registering or unsubscribing your recipients and it may not be a manual process either. Your e-mail templates will have to have a standard provision of containing an automatic de-register or unsubscribe link.

7 The identity and recognisability of the sender

The e-mail you send via Tripolis has to clearly show the identity of your organization. This might as a general rule include the company name in the From-name, for example. Moreover, the template should also contain the logo, the name (not a pseudonym) and the address details in question. It has to be clear to recipients immediately how they can contact you via e-mail (using an operational reply address) and also by telephone (by including a telephone number).

5 Dealing with and resolving complaints about spam

Tripolis may receive spam complaints from four parties which complaints may be cause for us to commence an investigation:

- Complaints from recipients or ISPs: we ask recipients or ISPs which specific e-mailing they are complaining about and the date thereof.
- Complaints from the Netherlands Advertising Standards Committee: recipients may also submit their complaints about spam to the Netherlands Advertising

Standards Committee. That body will then approach the sender and the advertiser (Tripolis user) in this connection.

- Complaints made to the official watchdog, the OPTA: when the OPTA receives multiple complaints and registers them about a specific e-mailing sent via Tripolis systems, the OPTA will then issue an official warning.
- Complaints from anti-spam companies: many private individuals and companies make use of anti-spam software which automatically deals with complaints. When a certain number of complaints are made, the companies which are behind the anti-spam software will send an automatic e-mail referring to the fact that the mail server of the sender of the spam has been temporarily black-listed.

If we receive a complaint about your e-mailings, we shall first come to you with the request for you to provide us with a written response, including proof of the opt-in, and make arrangements with you about how these problems can be prevented in the future. You are required to deal with complaints made concerning receipt of unsolicited e-mail in a correct and fully cooperative manner.

6 Measures

If that response and the solution found to the problem, sending unsolicited e-mail, is not received within 48 hours, we are entitled to deny you access to the Tripolis systems until we are convinced that the incident has been dealt with in full and measures have been taken to prevent sending unsolicited e-mail in the future.

We reserve the right to exclude you immediately from the Tripolis systems should it appear that you send spam. Our liability for consequential damage caused by sending spam on the part of the sender is excluded. Damage suffered by us in connection with non-compliance with this stipulation may be claimed by us as compensation for damage from the sender.

7 In conclusion

- Respect recipients! Give recipients the (relevant) information he or she asked for. Ensure that the content is technically in good order.
- Make sure your list is clean, process bounces, complaints and non-responses on a regular basis.
- Ensure for a well run and well organized infrastructure. Tripolis partners will be able to assist you with this. Think about implementing SPF, Sender ID, and Domain Keys/DKIM. An own IP address. Certification (for example, via Return Path).