E-Mail dispatch with myconvento

myconvento

E-Mail dispatch with myconvento

The successful dispatch of news to journalists, media, investors and other multipliers is one of the most important tasks of professional PR management. For this reason, we have developed a highly professional mailing system in close cooperation with our demanding users from the communications industry.

Standard or premium dispatch?

myconvento offers two basic distribution methods. The **Standard Dispatch** is completely sufficient for usual, traditional PR work. For Investor Relations, e-mail marketing and customer newsletters we recommend **Premium Dispatch**. The same applies to larger dispatch volumes and greater evaluation requirements.

Feature	Standard	Premium
immediate dispatch, scheduled dispatch, order without fixed dispatch time	✓	✓
any number of e-mail accounts, usable by any authorized users	✓	✓
any sender address, reply address, alias names ect.	✓	✓
delivery method Envelope, SPF und DKIM	✓	✓
recipients can be combined from own data and research databases	✓	✓
personal salutation in German, English and further languages	✓	✓
e-mail order in up to 5 languages parallel (selectable from 27 languages)	✓	✓
e-mail editor with templates for HTML and text version	✓	✓
design elements for designing the HTML body text	✓	✓
any number of attachments with any file formats	✓	✓
audit-proof archive of all messages	✓	✓
comfortable blacklisting und bounced mail handling	✓	✓
prioritized delivery within a few minutes		✓
evaluation „delivery rate“	**in detail**	**in detail**
evaluation „opening rate“	**in percent**	**in detail**
evaluation „click rate“	**in percent**	**in detail**
evaluation „click rate on external links“		**in detail**
„embedded pictures“ in HTML body		✓
display of your "Earned Media" after dispatch		✓
Drag & Drop-Editor		✓
monthly costs	**exceeding 2 GB 50 EURO***	**95 EURO***

* per every GB

myconvento

Distribution methods in myconvento

Envelope

With this method, the actual e-mail is packed in an "envelope". This identifies the technical sender, i.e. myconvento, and its client, i.e. the myconvento customer and ensures a technically correct dispatch. In the envelope of an e-mail sent by myconvento in this way, the technical sender mailservice@myconvento.com is therefore deposited. The advantage of this method is that the user can use the mailing system immediately. The disadvantage is that the recipient of an e-mail may see that the technical sender and the actual sender are not identical. Both may be visible to the recipient, depending on the e-mail client of the recipient.

SPF

In the SPF method ("Sender Policy Framework"), a special entry is made at the operator of the customer domain (a so-called DNS entry). This entry refers to the myconvento mail server and allows myconvento to send e-mails that seem to come from the customer. It is therefore a permission or authorisation.

The e-mail servers of the recipients recognize if the technical sender and the specified sender are not identical. They then use the DNS entry to check whether the sender has authorized the technical sender. If so, the incoming e-mail is not recognized as spam. It is therefore a technique for detecting and defending spam messages. At the same time, it helps legitimate senders to get through the spam filters and makes the technical sender invisible to the email reader.

DKIM

With DKIM, outgoing e-mails are signed. Private and public keys of the sender are used for this purpose. The receiving mail server can use the public key to verify that the message actually originates from the specified sender.

This ensures that the recipient does not technically perceive the e-mail as spam. DKIM is a relatively new alternative to SPF.

The differences between the three methods (illustrated by an example)

Suppose your name is XY and you want to send a postcard to the recipient YZ. The technical sender is Deutsche Post. You print your address and that of the recipient on the postcard. You take the postcard to the post office counter where it is put in an envelope and labeled with the remark "Sent to YZ by Deutsche Post on behalf of XY". That would be **Envelope**.

In the second case, you printed a stamp on the postcard before taking it to the post office. With this stamp, you authorise the Post to deliver the postcard for you. The recipient can read and understand this authorization. He can consult a publicly accessible directory in which you have declared the post to be one of your technical senders. That would be **SPF**.

In the third case, the stamp is unreadable because you encrypted it and thus made it illegible. However, the recipient can decrypt the content of the stamp using the public key which you made retrievable for him. This tells him that you are the sender, and that Deutsche Post is allowed to perform the dispatch for you. That would be **DKIM**.