



# **E-MAIL VERSAND MIT MYCONVENTO**

# E-Mail Versand mit myconvento

Die erfolgreiche Zustellung von Nachrichten an Journalisten, Medien, Investoren und sonstige Multiplikatoren gehört zu den wichtigsten Aufgaben eines professionellen PR-Managements. Aus diesem Grund haben wir in enger Abstimmung mit unseren anspruchsvollen Anwendern aus der Kommunikationsbranche ein hoch professionelles Versandsystem entwickelt.

## Standardversand oder Premiumversand?

myconvento bietet den Anwendern zwei grundsätzliche Versandarten. Der **Standardversand** reicht völlig für die übliche, traditionelle Pressearbeit. Für Investor Relations, E-Mail Marketing und Kunden-Newsletter empfehlen wir **Premiumversand**. Ebenso bei größerem Versandvolumen und größerem Auswertungsbedarf.

Feature	Standard	Premium
Sofortversand, zeitversetzter Versand, Auftrag ohne festen Versandtermin	✓	✓
beliebig viele E-Mail Konten, verteilbar auf beliebige Anwender	✓	✓
beliebige Absenderadresse, Antwortadresse, Aliasnamen usw.	✓	✓
Zustell-Verfahren Envelope, SPF und DKIM	✓	✓
Empfänger kombinierbar aus eigenen Daten und Recherche-Datenbanken	✓	✓
persönliche Anrede in Deutsch, Englisch und weiteren Sprachen	✓	✓
E-Mail Auftrag in bis zu 5 Sprachen parallel (wählbar aus 27 Sprachen)	✓	✓
E-Mail Editor mit Vorlagen für HTML- und Text-Version	✓	✓
Design-Elemente zur Gestaltung des HTML Bodytextes	✓	✓
beliebig viele Attachments mit beliebigen Dateiformaten	✓	✓
revisions sicheres Archiv aller Meldungen	✓	✓
komfortables Blacklisting und Bounced Mail Handling	✓	✓
priorisierte Zustellung innerhalb weniger Minuten		✓
Auswertung „Zustellrate“	<b>detailliert</b>	<b>detailliert</b>
Auswertung „Öffnungsrate“	<b>pauschal</b>	<b>detailliert</b>
Auswertung „Klickrate“	<b>pauschal</b>	<b>detailliert</b>
Auswertung „Klickrate auf externe Links“		<b>detailliert</b>
„embedded pictures“ im HTML Body		✓
Übertragung von Word-Dokumenten nach HTML		✓
monatliche Kosten	<b>über 2 GB 50 EURO*</b>	<b>95 EURO*</b>

\* je angefangenes Gigabyte

# Zustellverfahren in myconvento

## Envelope

Bei diesem Verfahren wird die eigentliche E-Mail in einen „Umschlag“ gepackt. Dieser identifiziert den technischen Versender, also myconvento, und seinen Auftraggeber, also den myconvento Kunden. Dadurch gewährleisten wir, dass wir technisch einwandfrei versenden können. Im Umschlag einer E-Mail, die von myconvento nach diesem Verfahren versendet wird, ist folglich der technische Absender mailservice@myconvento.com hinterlegt. Der Vorteil dieses Verfahrens ist, dass der myconvento Anwender das Versandsystem sofort nutzen kann. Der Nachteil ist, dass der Empfänger einer E-Mail unter Umständen sehen kann, dass der technische Versender und der eigentliche Absender nicht identisch sind. Beide sind unter Umständen – je nach Client des Empfängers - für den Empfänger erkennbar.

## SPF

Beim SPF-Verfahren („Sender Policy Framework“) wird beim Betreiber der Kunden-Domain ein spezieller Eintrag vorgenommen (ein sogenannter DNS-Eintrag). Dieser Eintrag verweist auf den myconvento Mailserver und erlaubt myconvento, E-Mails zu versenden, die scheinbar vom Kunden kommen. Es handelt sich also um eine Erlaubnis oder Autorisierung.

Die E-Mail Server der Empfänger erkennen, wenn technischer Versender und angegebener Absender nicht identisch sind. Sie prüfen dann anhand des DNS-Eintrags, ob der Absender den technischen Versender autorisiert hat. Wenn ja, wird die ankommende E-Mail nicht als Spam wahrgenommen. Es handelt sich also um eine Technik zur Erkennung und Abwehr von Spam Nachrichten. Gleichzeitig hilft sie rechtmäßigen Versendern, durch die Spam-Filter zu kommen, und macht für den Leser der E-Mail den technischen Versender unsichtbar.

## DKIM

Bei DKIM werden ausgehende E-Mails signiert. Dazu dienen private und öffentliche Schlüssel des Absenders. Der empfangende E-Mail Server kann mit Hilfe des öffentlichen Schlüssels feststellen, dass die Nachricht tatsächlich vom angegebenen Absender stammt.

Damit ist sichergestellt, dass die E-Mail vom Empfänger aus technischer Sicht nicht als Spam wahrgenommen wird. DKIM ist eine relativ neue Alternative zu SPF.

## Die Unterschiede der drei Verfahren an einem Beispiel

Nehmen wir an, Sie heißen XY und wollen dem Empfänger YZ eine Postkarte zusenden. Technischer Versender ist die Deutsche Post. Auf die Postkarte drucken Sie Ihre Adresse und die des Empfängers. Sie bringen die Postkarte zum Postschalter, und der Beamte steckt sie in einen Umschlag und beschriftet diesen mit dem Satz „Versendet an YZ von der Deutschen Post im Auftrag von XY“. Das wäre **Envelope**.

Im zweiten Fall haben Sie noch einen Stempel auf die Postkarte gedruckt, bevor Sie sie zum Postamt bringen. Mit dem Stempel autorisieren Sie die Post, für Sie die Postkarte zuzustellen. Der Empfänger kann diese Autorisierung lesen und verstehen. Er kann dazu in einem öffentlich zugänglichen Verzeichnis nachsehen, in dem Sie die Post zu einem Ihrer technischen Versender erklärt haben. Das wäre **SPF**.

Im dritten Fall ist der Stempel unlesbar, weil sie ihn verschlüsselt und damit unleserlich gemacht haben. Der Empfänger kann aber mit Hilfe des über Sie abrufbaren öffentlichen Schlüssels den Inhalt des Stempels entschlüsseln. Damit erkennt er, dass Sie der Absender sind, und die Post für Sie versenden darf. Das wäre **DKIM**.

