BEST PRACTICES
FOR EMAIL MARKETING

Authors: Marius Bauer, Mathias Ullrich, Florian Vierke

ASSOCIATION OF THE INTERNET INDUSTRY

Content

Introduction

Reputation concept

No deliverability guide is complete without the term 'reputation'. Put simply, reputation is a metric that indicates how well a sender is regarded. But what seems like a simple metric at first glance quickly turns out to be very complex. Unfortunately, there is no such thing as 'the' reputation. Each mailbox provider works with different data and sets different priorities. This results in different reputations per mailbox provider, sometimes even split into IP and domain reputation.

Risks

The risks in email marketing are mainly related to legal challenges, especially since the introduction of the General Data Protection Regulation. And, of course, the legal risk is especially present in Germany and cannot be ignored. More about what data collection should look like later. But this is not the only risk. The goals of email marketing are usually clearly defined and, thanks to modern sending and tracking systems, also very easy to track, such as turnover or impressions on the homepage. To achieve these goals, however, it is essential that the emails actually reach the recipients' inboxes. An email in the spam folder rarely generates sales; this document is intended to help minimise this risk, in particular.

Spam filters or legislation: Who decides?

In our work, we often come across variations of "but it's legal". Which leads to the question of whether it should be the spam filters of email providers or the legal framework that determines what constitutes good email marketing.

Given that there is a huge patchwork of laws and regulations around the world governing 'electronic advertising', one can almost be glad that the rules of spam filters or mailbox providers determine the deliverability of an email, because while there are slight varia - tions, the direction is the same for almost all legitimate providers.

As mentioned in the risks section, an email that has been moved to the spam folder by the provider does not generate any revenue. And since there is no legal right to delivery to the inbox, the spam filter is the ultimate arbiter.

Who does what – service provider or sender?

Email marketing is often carried out in a 'service provider'and 'sender' constellation, which naturally raises the question of who is responsible for what. This always depends on the scope of the service provider's offering, but the basic rule is that the content and data are the responsibility of the sender, and the technology lies with the service provider.

And that's where an important element of deliverability lies, because you can do very little to fix problems on the service provider side. If messages end up in the SPAM folder, it is possible to work with the service provider to find solutions. But it is the responsibility of the sender to implement them.

Before dispatch: Contents

Data quality & collection

Email marketing stands and falls with the data. This begins with the clean collection of data, continues with the regular maintenance of address data and ends with the unsubscription of addresses.

Data collection

Even if the legal framework does not set the rules for email marketing, legally compliant data collection is mandatory. Not least because the German regulations, in particular, are very close to what mailbox providers expect from senders.

Active and transparent consent is at the heart of data collection. Even before the EU General Data Protection Regulation (GDPR), consent was the golden way to generate recipients. But not all consent is the same, which is why the adjectives 'active' and 'transparent' are so important.

In order to meet the legal requirements, some marketers try to hide consent in the privacy policy or work with pre-selected checkboxes. But this approach is neither sustainable nor successful.

Active in the context of consent means that the recipient takes an intentional action to consent. This could be clicking a button or ticking a checkbox.

Transparent also means that the potential recipient knows exactly what to expect before taking action. Ideally, all information such as the frequency of sending, what content will be offered, how to unsubscribe, etc. is available.

Particularly in the DACH region, double opt-in has become established as an additional aspect of data collection. The DOI is also known as 'verification'. It ensures that the owner of the email address is the same person who gave consent. The DOI is also recommended by German data protection authorities.

Another common practice is to add existing customers to the pro - motional mailing list. This is allowed in Europe, but with high legal hurdles. It is important to be as transparent as possible when col - lecting data about the possibility of opting out, to only advertise similar products and, of course, to take existing unsubscriptions into account. It is also advisable to obtain consent for online orders.

For more information on how to structure consent, contact your in-house counsel or the CSA, which recently updated its legal guide – the Directive for Permissible Email Marketing - in its 7th edition.

Database hygiene

Of course, data collection is not the end of the story. Anemail distribution list needs constant maintenance to ensure maximum success. This includes, on the one hand, removing subscribers who have unsubscribed and recipients who are no longer active (more on this in the chapter on dispatch follow-up), but also implementing a strategy for removing inactive recipients.

Writing to recipients who do not interact has a negative impact on delivery success. These should therefore be removed regularly, ideally automatically. Typically, this is done based on opens, clicks or other metrics. The appropriate time period will vary from brand to brand, but in most cases 12 months is a good period.

Email validation services

There are several providers of so-called validation services on the market, which try to ensure the authenticity of an email address in various ways. These services typically offer two different models:

On-demand validation

This is where a validation is performed directly during data col lection (both online and offline) and alternatives are suggested in case of possible errors. For example, 'typos' can be corrected before the email address turns out to be incorrect.

The cost, which may not be justified in every application, is usually a disadvantage of this option.

Lists validation

This model examines existing lists and makes recommendations as to what should be done with which addresses.

In most cases, this process is not too expensive, but expectations of the results are sometimes exaggerated. For example, it should be remembered that such a process cannot verify consent, and the subsequent modification of records is also legally questionable. Identifying and removing spam traps (see next chapter) is also more complex than providers sometimes make it seem.

On-demand validation may be recommended if the value of an individual email is high enough to justify the cost.

Spam traps ('Recycled' and 'Pristine')

The term 'spam trap' is often used when discussing the quality of address lists. Spam traps are email addresses that do not "belong" to any natural person, but are operated by various companies to identify senders who send unsolicited mailings or do not maintain their records. There are two main categories of spam traps:

Recycled Traps

These email addresses once belonged to users but were abandoned at some point, so the mailbox provider takes them over and uses them as spam traps after a transition period. This makes it possible to identify senders who have no bounce management or who are writing to old addresses.

Pristine Traps

These spam traps were never anything other than spam traps. While it is possible for recycled traps to have once given consent, this is impossible for pristine traps. If such email addresses are being used, this indicates a problem with the data collection.

Spam traps in mailing lists are not uncommon, and most spam traps do not directly affect deliverability. However, spam traps are always a strong indicator that best practices are not being followed, which can lead to problems. It is therefore important to eliminate spam traps at an early stage.

Unfortunately, it is not possible to identify spam trapsdirectly, as they are trade secrets of the providers and mailbox providers. However, it is important to ensure that these spam traps do not show any engagement. Therefore, spam traps should be removed directly when inactive recipients are purged.

Engagement as the key to the inbox

'Engagement', like 'reputation', is a term that is difficult to define as each email provider handles it differently.

Generally speaking, engagement is any interaction on the part of the recipient. A broad distinction is made between positive and negativeengagement.Positiveinteractionsincludeopening,clicking, replying and 'fishing out' of the spam folder, while negative inter - actions include 'deleting unread' or 'marking as spam'.

And these are just the most obvious options. It is likely that mailbox providers are analysing their users' behaviour much more closely.

They use this knowledge to decide which emails get into the inbox and which do not. The higher the provider estimates the relevance of an email to the user, the more likely it is to be delivered to the inbox.

So marketing goals and delivery success go hand in hand, because positive engagement is always the goal.

And that goes for the content of the email as well. We can't make any specific recommendations here, because every sender is a little different, starting with big differences like B2B vs. B2C, and continuing with different marketing goals, target audiences, product ranges, etc.

However, the focus must be on encouraging the recipient to engage as positively as possible, on subject lines that encourage people to open the email, on content that is interesting to the recipient and ideally leads to a click.

That way, when the next email arrives, the mailbox provider knows that the user is interested in that content and the email willbe delivered to the inbox.

What is an opening?

This question may sound banal, but in the age of Google Cache, Yahoo Image Proxy or Apple's Mail Privacy Protection (MPP), it makes sense to take a closer look here.

First of all, a distinction must be made between what the marketer and what the mailbox provider understand by an opening. For the provider, an opening is just that: the active action of the user to open an email. Since this information is not public, an opening is not clear for marketers.

To find out whether a recipient opens an email, marketers use the trick of the 'opening pixel' with the help of their technical service providers. This is a transparent GIF in the size 1x1 pixel. If this GIF is loaded, e.g. because an email is opened, this is noted as an opening. However, this is not an exact metric, because on the one hand it is possible to open an email without loading an image, and on the other hand it is possible for the mailbox provider to load the image without the user taking action.

This is exactly what happens with Apple's MPP. This was introduced with iOS 15 and when it is activated, the email client loads the images in the background when the email arrives. This also loads the open pixel so that the open rate appears higher than it actually is.

This means that the open rate as the sole metric may no longer be the measure of all things, but together with other KPIs it is still a useful reporting tool.

Inbox placements

When Gmail introduced the different 'tabs' in 2013, there were fears that emails in the 'Promotions' tab would go unnoticed. Tactics quickly emerged to ensure that Google would not recognise the ads as such. There are no such tactics here, so are the tabs a problem at all?

Probably the most important aspect is that all tabs are in the inbox. Messages in the Promotions tab have not 'disappeared'; they are where the user expects to find commercial emails. In addition, current estimates suggest that only about 20 percent of Gmail users have tabs enabled. In addition, Gmail apps do not support tabs.

Taken together, these factors suggest that advertising messages should be delivered in the Promotions tab, as this is what users who use the tabs expect. In addition, the Promotions tab offers the opportunity to use additional features such as 'annotations'.

During sending:
Technical sending basics

Authentications

One of the most important requirements for successful bulk emailing today is the correct authentication of the sender domain. In other words, the sender must prove that they are authorised to send on behalf of the display-from address (also known as RFC 5322. FROM). This requirement was not included in the original email standard and there are still many mail servers that accept email without authentication.

However, as part of the fight against phishing and abuse,most major Internet Service Providers (ISPs) have made it a requirement that mailings are also correctly authenticated.

There are two technical methods of authentication: SPF (Sender Policy Framework) and DKIM (Domainkey Identified Mail).

Implementing both is strongly recommended as many receiving mail servers only check one of the two methods. Furthermore, you will still be securely authenticated even if one of the two methods fails for technical reasons.

SPF (Sender Policy Framework)

With SPF it is possible to store in the DNS (Domain Name System) of the Envelope From domain (5321.FROM) via a TXT entry which IPs are valid for sending and which are not. In this way, the receiving mail server can very quickly determine whether a message actually comes from the specified server.

SPF is very easy to implement and does not use any additional resources when sending. Unfortunately, it has some weaknesses,
which is why most ISPs prefer DKIM authentication – or even ignore SPF altogether. Nevertheless, SPF should be implemented.

The main drawbacks of SPF are

- SPF fails when email is forwarded: The receiving mail server checks the IP address of the forwarding mail server, not the IP address of the original sender. For example, SPF fails when using mailing lists.
- SPF cannot identify a single sender domain. Many infrastructures use 'shared IPs', i.e., the same IPs are used for several mail domains. Even if the provider changes, the IP cannot be taken with them. The relevance of IP reputation compared to domain reputation is therefore decreasing.

DKIM (DomainKey Identified Mail)

With DKIM, authentication can be implemented at the domain level. This makes it very attractive and unavoidable in practice.

Technically, a pair of keys is generated for DKIM, usually using the RSA method and a key length of 1024 or 2048 bits. The private part of the key generates a signature that is included in the email header. The public part of the key is stored in the DNS so that the receiving mail server can check the signature of incoming messages for validity. The trick is that the signature contains information about the relevant header fields, ensuring that the header has not been altered or forged since it was sent. Valid signatures can therefore only be created by people who have the private key that matches the public key in the DNS.

TLS (Transport Layer Security)

TLS (Transport Layer Security) is a protocol designed to securely transfer data over the Internet. Encryption is performed using asymmetric keys consisting of a public key and a private key.

Even today, some mail servers will not accept mail that is not sent via TLS (especially bulk mail). In practice, TLS versions 1.2 and 1.3 are used almost exclusively; from 2021, the use of TLS 1.1 (or lower) has been discouraged.

DMARC (Domain-based Message Authentication, Reporting & Conformance)

DMARC is a standard that allows senders to inform the receiving mail server of a policy for handling unauthenticated mailfrom their own domain. The methods available are 'none' (no filtering), 'quarantine' (filtering of unauthenticated mails to the spam folder) and 'reject' (rejection of unauthenticated mails).

Authentication can be done using SPF or DKIM. The prerequisite for this is that the respective domains are 'aligned', i.e. belong to the same domain.

For example, if I want to use DKIM to authenticate an email from 'foo.com' in the DisplayFrom (5322.From) field, my email must contain a valid DKIM signature from the foo.com domain. Subdo - mains are allowed in both the signature and the From field, unless the policy is explicitly configured for 'strict' alignment. For the standard case, 'relaxed' alignment is sufficient.

On the other hand, if I want to authenticate a mail from foo.com via SPF in the Display From (5322.From), I must both pass a valid SPF check and use the domain foo.com in the Envelope From. Again, subdomains are allowed by default.

DMARCalsoallowsyoutospecifyanemailaddresstoreceivereports on the filtering of emails received by the recipient. Once enabled, reports are typically received daily from any recipient domain that sends DMARC reports. These reports are in machine-readable XML format and should be graphically displayed using a tool or service. Free open-source software is available from parseDMARC (https://domainaware.github.io/parsedmarc/), but there are also commercial providers that do not require you to host your own server.

BIMI (Brand Indicators for Message Identification)

Most email marketers associate the term BIMI with the possibility of placing their own company logo as a sender image in email cli - ents. However, the actual idea behind BIMI goes far beyond the logo. It is about presenting brand communication as such only if the mailings were actually sent by the brand.

The prerequisite for this is that brands have registered their logo as a figurative mark with an official body (e.g. the German Patent and Trademark Office). Furthermore, it is necessary to verify the domains used and the company as such. A so-called 'Verified Mark Certificate' (VMC) serves this purpose.

The dispatch must also be correctly authenticated. Asuitable technology is already available for this with DMARC. The prereq- uisite for displaying the BIMI logo in email clients or email apps is setting up DMARC with a policy of 'quarantine' or 'reject' on the client's domain.

Currently (as of February 2025), BIMI is supported in conjunction with a VMC certificate by the following major providers: Gmail, Yahoo, AOL, Apple (Mail app on iOS). BIMI is also supported by au.com, Cloudmark, Fastmail, Laposte, 1&1, Onet, Zoho and Zoner (https://bimigroup.org/bimi-infographic)

Dispatch follow-up: Data follow-up, response handling

Data quality & maintenance

Just as important as the correct collection of data, including consent, is a responsible and conscious approach at the 'other end' of the customer lifecycle. The number of email recipients is an impressive but not very meaningful indicator. What is more important is the level of engagement of the respective target groups. After all, as mentioned above, it is the recipient's interaction with the content that determines the sender's reputation. In a nutshell: Be relevant. Always. Mailings are only sent to those who have specifically requested them. No one stays in the database longer than necessary.

Bounces

The term 'bounces', borrowed from the postal system, is still in use today. Bounces are the total number of emails that have been sent but not delivered. There are many reasons for this. It is advisable to implement specific measures for the different types of bounces (see below) or to ask the technical sender (ESP) about the on-board means and the setting options on their platform.

Hard bounces

If an address does not exist, the sending platform will report a hard bounce based on the feedback from the Internet service provider.

An address is not available:

- The domain exists, but the user does not.

In principle, hard bounces should disappear from the active recipient list immediately, ideally after the first incident.

Soft bounces

If there is a possibility of reaching the recipient again in the future, this is called a soft bounce. Common examples are:

- Mailbox full:
  There is no more storage space available for the user to accept the email. If the mailbox is emptied in the future and the user frees up space, this status changes and emails can be accepted again. The problem is pushed down the road. Today, gigabytes of storage are often already allocated to free user accounts. It is therefore likely that this type of bounce is preceded by a very long period of inactivity.
- Spam reject:
  Rejection due to suspected spam may be based on the reputation of the domain/IP or the message itself. In many cases, such rejections are also blanket for all customers of a mailbox provider. A negative reputation is reversible. So, with an appropriate response to such an incident, deliverability will also be restored. It is important to distinguish between personal and ISP-wide rejections. Some providers provide information on whether the rejection is based on a general decision (filter, gateway or reputation rejection) or a personal decision (user rejection).
- Automatic reply / autoresponder:
  This delivery error is caused by auto-reply messages, such as an out-of-office message sent by an autoresponder. You can disable contacts after a certain number of auto-replies to avoid sending too many messages to contacts who are absent for a long period of time. Many senders offer the ability to 'intercept' such non-bounces through their platform. The success rate is close to 100%.
- Communication failed:
  This delivery error is caused when no connection could be established to the receiving mail server (MTA).
- Invalid:
  This bounce is generated when the domain of the email address does not exist (e.g. hotnail.com instead of hotmail.com) or the domain could not be resolved due to DNS problems at the ISP. The following bounce category is used when the exact reason for the failed delivery cannot be determined. Depending on the service provider and platform, designations such as 'Unknown', 'Other' and others are also possible.
- Other:
  There are many other reasons why messages may not be accepted. These should be reviewed on a case-by-case basis and, if necessary, added to an automated processing routine. It is always worth talking to the service provider to improve the mapping on an ongoing basis.

Automatic and timely processing of bounces is essential.Some email service providers also offer automatic reactivation for soft bounces. Ideally, the ESP of choice will provide an automated de- and reactivation routine. This should be tailored to your specific send behaviour.

Temporary bounces

During the sending process, a mailbox provider can also delay the acceptance of emails. This is usually seen as a precursor to actual blocking. The larger providers on the market also justify such 'delays' in server communication as 'reputation-related'. This practice has its origins in so-called greylisting. It is important to know that (real) spammers are extremely resource efficient. This means that they only make one delivery attempt per recipient and then immediately 'give up'.

A technical delivery service provider usually configures the mail servers so that several delivery attempts are made before the attempts are cancelled after a defined period of time. This means that if reputation declines overtime, delivery delays can occur long before open and click-through rates start to drop or bounce rates start to rise.

Deregistrations

An unsubscribe is a friendly form of negative evaluation of a mar - keting communication. An active newsletter recipient is no longer interested in the content and unsubscribes for the future. This is annoying, but part of the everyday life of every email marketer. However, unlike soft bounces, unsubscribes leave no room for nego - tiation or interpretation. Often the unsubscribe link is small and inconspicuous. Accidental clicking can therefore be ruled out with some certainty. There are various ways of allowing the recipient to remain on the mailing list. Preference centres are often used. These can offer unsubscribe options by newsletter category or fre - quency adjustments. It is important to avoid making it difficult to unsubscribe. For example, asking for the email address in an empty form, sending an email to confirm the unsubscription with a single click (double opt-out) or requiring a login to the user profile can significantly increase the likelihood of a complaint.

Complaint feedback loops

Marking an email as spam is the easiest way for a recipient to remove emails with unwanted content or from unwanted senders from their inbox. Once a user complains about spam, the mailbox provider moves all future messages from that sender to the spam folder.

In order to minimise the volume of unwanted email that needs to be processed, many mailbox providers have adopted the practice of informing the technical sender of an individual recipient's com - plaint. This is done in the expectation that the sender will then stop sending spam.

The technical solution is as follows: In the event of a complaint, the receiving mailbox provider sends an email back to the technical sender (ESP) in a specific format. This email contains all the necessary information for the sender to identify the recipient and not to contact them again. As a result, no furtherpromotional emails will be sent to this sender in the future.

Transactional emails that are triggered by the complainant at a later point in time, e.g. as part of an order process, are excluded from this policy.

For example: If max.mueller@example.com complains about the promotional email on Monday and then orders an item on Wednesday, the order, shipping and payment confirmation can and must still be delivered.

In general, complaints that are not addressed in a feedback loop can have an extremely negative impact on a sender's reputation.

Manual answers

Email is a dialogue tool, so email newsletters are classified as dia - logue marketing. Consequently, responses from recipients should not only be technically possible, but also expected.

Avoid 'no-reply@' sender addresses, as these suggest that a response is not desired.

Use the mailing service provider's experience and capacity to filter out automatic replies and process unsubscribes from emails so that, where possible, only actual replies from recipients are passed on to customer service.

About the authors

Florian Vierke
Senior Manager, Deliverability Services | mapp

Marius Bauer
Senior Deliverability Consultant | Salesforce

Mathias Ullrich
Deliverability Services Consultant | Adobe

Florian, Marius and Mathias have each been working as email deliverability experts on the side of technical mailing service providers for over 12 years. They see association work as an integral part of their mission to help senders evolve their email communication strategies. Their common desire for (really) everyone to be able to send better emails is reflected in this guide.

Your point of contact at eco for the topic of email:

Michael Weirich

IT Security Project Manager
eco – Association of the Internet Industry Lichtstrasse 43h
50825 Cologne
Germany
Phone: +49 (221) 7000 48 – 193
Mobile: +49 (0)171 – 554 0303
Email: michael.weirich@eco.de

BEST PRACTICES
FOR EMAIL MARKETING

Authors: Marius Bauer, Mathias Ullrich, Florian Vierke

eco – Association of the Internet Industry
Lichtstrasse 43h, 50825 Cologne
phone +49 (0) 221 / 70 00 48 – 0
fax +49 (0) 221 / 70 00 48 – 111 info@eco.
de
international.eco.de

ASSOCIATION OF THE INTERNET INDUSTRY