valid for

D A CH

eco Directive for Permissible e-Mail Marketing

Guidelines for Practical Use
6th edition 2016

UPDATED worldwide Opt-In/Opt-Out-List!

Edited by

CSA
Certified Senders Alliance

eco
ASSOCIATION OF THE INTERNET INDUSTRY
WE ARE SHAPING THE INTERNET.
YESTERDAY. TODAY. BEYOND TOMORROW.

INDEX

Content

1. Foreword

In 2002, the online marketing competence group of eco – Association of the Internet Industry adopted the first "Directive for Solicited Online Marketing". Since then, the Directive has been updated on a regular basis and more than a million copies of the popular guidelines were distributed or downloaded as a PDF from the eco website.

The current revision of the Directive takes into account a series of recent judgments (e.g. the judgment of the German Federal Court of Justice on automated email responses). Noteworthy are the consequences of the new EU General Data Protection Regulation applicable from 25 May 2018 on. This applies directly and immediately and no longer needs to be transposed into national law in each case. Illegal advertising methods and data protection violations can then be sanctioned with drastically increased fines of up to EUR 20 million.

The extensive list of countries for which the legal basis of email marketing is explained has been supplemented. The chapters on the legal situation in Austria and Switzerland have been expanded.

Email marketing continues to be a fixed part of the customer communication of many companies. In order to further clarify the special circumstances with regard to the legal conformity of this marketing communication, specific and practice-oriented instructions for action are given in these guidelines. The present Directive gives companies an answer to the most frequent legal questions. There are three areas for each question:

1. Legal requirements
2. An explanation of the question and recommendations for the practical implementation of the statutory requirements
3. Practical examples

The most pressing legal issues from a company perspective relating to the sending of emails are:

- Have the recipients given their consent?
- Can the consent be proven?
- Do the recipients know what they have consented to?
- Were the recipients informed about the unsubscribe option, which must also be able to be implemented free of charge and without any difficulty?
- Do the recipients receive an email confirmation of their consent?
- Are enquiries responded to?
- Is the subject not misleading?
- Is the sender clearly discernible?
- Is the legal notice complete?
- Does it involve a case of contract data processing and have the corresponding statutory regulations been complied with?

Of course, this Directive cannot replace any legal advice in individual cases. However, it can help to ensure that companies feel more confident when they use email or direct marketing as a communication medium when in contact with interested parties. Consumers should also be able to feel safer when they provide a company with their email address. Safe means that addresses are not simply forwarded, that emails can only be sent with the addressee's consent, and that it is easily possible to have one's own address deleted

from a distribution list again at any time.

The great success of email as a communication medium is based on trust. This Directive should contribute to helping companies create and maintain trust. The Directive can also be retrieved online at **https://certified-senders.eu/documents**.

2. Permission

It is now generally known that advertising by email fundamentally requires the consent of the recipient, both in the B2C area and in the B2B area. The requirements of valid consent can be summarized in brief as follows:

- transparent
- voluntary
- conscious, clear, explicit, and
- separate

In addition, it must be possible to prove consent and to record it in detail. For email advertising within the framework of existing customer relationships, the law makes provisions for certain alleviations (cf. Chapter 2.12).

2.1 Legal basis

At the European level, the Directive on Privacy and Electronic Communications (also known as E-Privacy Directive) already provides in Section 13 that the consent of the addressee is required for the sending of email advertising. This statement is valid for all EU Member States alike. However, EU directives are not directly applicable, but must be transposed into national legislation in each individual EU Member State. This transposition into national law often results in considerable legal differences. Also, there are also variations in the ways that national courts and data protection supervisory authorities interpret laws. This leads to the fact that, although the right of email marketing has a single European basis, some differences in the details can still be established (see also the overview of the legal situation in different countries in Chapter 10).

The guidelines of the European Union for email advertising are transposed into national law in Germany by the BDSG (Bundesdatenschutzgesetz [German Federal Data Protection Act]), the TMG (Telemediengesetz [German Telemedia Act]) and the UWG (Gesetz gegen den unlauteren Wettbewerb [Federal Act Against Unfair Competition]). The requirement for consent to email marketing results from Section 7 para. 2 UWG and from Section 28 para. 3 sent. 1 BDSG.

Although the principle of "Email Advertising only by Consent" may sound simple, its specific implementation is difficult. Through numerous rulings and amendments to laws, the requirements for legally effective declarations of consent are also being modified constantly (and usually tightened).

A future amendment of the legislation is already imminent: the EU General Data Protection Regulation.

The new EU General Data Protection Regulation, which will enter into force on 25 May 2018, is directly and immediately applicable and no longer needs to be transposed into national law in each case.

It intends, among other things, to harmonize the data protection legislation in the EU. From a German point of view, the legal basis for consent and the admissibility of email advertising remains on the whole. However, illegal advertising methods can be sanctioned with drastically increased fines. The level of fines for data protection violations will increase up to EUR 20 million or 4% of a company's total annual sales achieved worldwide (depending on which is higher).

2.2 Definition of advertisement

The consent of the addressee is required for the sending of email advertising. Here, the question arises with regard to what qualifies as an advertisement from a legal perspective.

Legislation and case law are less scrupulous when it comes to what should be seen as advertising. Any statement that is used directly or indirectly to sell products or services falls under the term "advertising". As lawyers put so succinctly, the term "advertising" can be "interpreted in many ways". For instance, case law also considers birthday or Christmas greetings in emails from a company to its customers and emails for a market research study that is not carried out on a neutral basis, but in the interest of a company, to be advertising. Almost everything that a company does and communicates externally ultimately serves to sell products or services. This also includes, for instance, the so-called solicited advertising or pure image advertising (advertisement of a trade mark without reference to a specific product), as well as the so-called service messages with information on other products, because even with these, turnover is indirectly promoted. Election advertising of political parties and donations for advertising of non-profit organizations also fall under the concept of advertising.

2.3 Transparent consent

Valid consent must meet certain requirements with regard to form and content. It is crucial firstly that the consenting party is informed in a transparent and easy-to-understand manner about the content of his or her declaration of consent. According to Section 4a para. 1 sent. 2 BDSG and the adjudication of the Federal Court of Justice (BGH) on 25 October 2012, File Ref. I ZR 169/10, consent is only valid when it is declared in full knowledge of the circumstances and for the specific case. The consenting party must be able to clearly identify who can use his or her data and for what purposes.

The company that intends to refer to the consent in the future must be clearly named. The consent always applies only for the company explicitly named. There is no "blank consent" that, for instance, could entitle a company XY and its "partner companies" to conduct email advertising. The data protection law also does not make provision for group privilege. Nor is forwarding of email addresses within the group for advertising purposes of other group companies permissible (if the group companies are not expressly named in the consent). A general naming of company XY "and affiliated companies" may also constitute a breach of the requirement of transparency.

The content of the future advertising emails should also be addressed as transparently as possible in the declaration of consent. If, for instance, a company markets various product lines under different brands, the declaration of consent should indicate whether the addressee will receive advertising exclusively for the product line under the brand X in the future or whether all the company's brands will be advertised.

Worst practice/negative examples:

☐ *I consent to my data being used for advertising purposes. I can revoke my consent at any time by sending an email to unsubscribe@abd.com.*

Such a declaration of consent is invalid as it is not discernible here which media (email, SMS, telephone, letter) are to be used for advertising.

☐ *I would like to receive advertising from ABC Co. and from the partner companies of ABC Co. by email. I can revoke my consent at any time by sending an email to unsubscribe@abc.com. In addition, a link to unsubscribe from other information is included in each email.*

This declaration of consent does not inform the addressee about which partner companies are involved. The consenting party thus has no idea what companies his or her email address will be forwarded to. In the case of consent which also includes the forwarding to third parties, the potential recipients of the data must be named in detail.

2.4 Conscious, clear, and explicit consent

Pursuant to Section 7 para. 2 no. 3 UWG, consent must explicitly be given by the consenting party, i.e. in a conscious and active manner. This can be done in writing with the signature of the consenting party or in electronic form by clicking on a check box. An opt-out option, i.e. for instance a check box that can be clicked when no email advertising is wanted, or a pre-clicked check box therefore do not constitute valid declarations of consent. The publishing of the email address in public directories, on the Internet page, in a letterhead, or on a business card does not constitute consent to the sending of email advertising either. A presumed or implied consent with which interest on the part of the addressee is merely assumed is no longer sufficient.

Consent to the sending of email advertising must always also be given separately, i.e. it cannot be combined with other declarations. For the confirmation of a purchase in an online shop ("Order now with costs") on the one hand and the consent to email advertising on the other, two separate check boxes must thus be provided. The BGH once again reaffirmed this in its judgment in the so-called "Payback Judgment" (Judgment from 16 July 2008, File Ref. VIII Civil Law Case 348/06).

The wording of the declaration of consent must clearly indicate that a consent is granted. For example, the wording "I know that ..." is not enough because the consenting party here is not necessarily aware that he or she is making a declaration of consent. The Düsseldorfer Kreis [Düsseldorf Working

Group of the Conference of Independent Federal and State Data Protection Authorities] makes reference to this in its helpful guide for the data protection declaration of consent in forms (only available in German) from March 2016.

Worst practice/negative example:

I would NOT like to receive the email newsletter of ABC Co.

The "opt-out" in this case does not constitute a valid declaration of consent. The consent must be given by active measures by the consenting party. Here, however, the consenting party must become active if he or she does not want to give his/her consent.

Best practice/positive example:

☐ *I would like to receive the weekly newsletter of ABC Co. with information on its offers from the field of telecommunications by email. My data will not be forwarded to third parties under any circumstances. I can revoke my consent at any time by sending an email to unsubscribe@abc.com with effect for the future. In addition, a link to unsubscribe from other information is included in each email.*

This declaration of consent meets the statutory requirements.

2.5 Formal requirements of the consent

Consent by postcard or letter: As a fundamental rule, consent must be given in writing (Section 4a para. 1 sent. 3 BDSG). By "in writing", the law means the handwritten signature of the consenting party. Therefore, if consent is given in a document – for instance, a postcard or letter – which the subsequent addressee of the advertising email has signed, the consent can be proven by this document. For this purpose, it must be ensured that the document is retained.

Online consent: On the Internet, consent can also be given in electronic form. Pursuant to Section 13 para. 2 TMG, electronic consent must also meet some formal requirements, i.e.:

- the consent has to be recorded,
- the user must be able to retrieve the content of the consent at any time, and
- the user has to be able to revoke the consent at any time with effect for the future. This right of revocation is to be pointed out to the user beforehand (Section 13 para. 3 TMG).

Consent through personal contact and on the telephone: Consent can also be given on the telephone or in person, for instance during a call to a call center or "face-to-face" at a trade fair. Since the reform of the Data Protection Act in 2009, however, such consent, which is not granted in writing or electronically within the meaning of Section 13 TMG, must be confirmed in writing (Section 28 para. 3a BDSG).

2.6 Data economy

Under the consent, no more data may be requested from the recipient than are actually necessary for the provision of the service. Usually, only a request for the email address is necessary for the sending of an email newsletter. The obligatory request for the first name or surname to personalize the email newsletter is not seen as permissible by all data protection supervisory authorities. However, as many items of data as required can be requested and given on a voluntary basis.

2.7 Co-registration and purchase of addresses

With the acquisition of address data for third parties (lead generation through co-registration), the companies for whom the addresses are to be collected must be named in detail as well. At the same time, the number of companies for whom addresses are to be collected should be manageable. In particular, it is recommended that the following requirements be met:

- The companies for whom the address data are to be generated must be specified individually by name and with indication of the sector.
- It must be possible for the user to take note of the list of companies easily and clearly within the consent process.
- The size of the list is restricted to a maximum of ten (10) companies.

The threshold of manageability may at any rate be exceeded if the user can no longer recognize the participating companies "at a glance".

The use of purchased email addresses entails increased due diligence obligations. Since according to case law, the purchaser of the email addresses must ensure that the owner of the respective email address is really in agreement with the sending of the advertising and that the legally effective submitted consent refers in particular not only to the mailing by the seller, but also by third parties (in this case the purchaser). In this case, it is not sufficient to rely on the assurance from the seller that the consent had been given. The purchaser must have been provided the corresponding documented records and must at least carry out a random check. That is, in order to take the most reliable path in this area, the records of consent should not only be shown but also stored in the company's own files for documentation purposes.

2.8 Consent of minors

The minimum age for the ability to give consent is not clearly defined. Within the framework of email advertising, minors aged 16 and over can generally be seen as capable of giving consent. However, in the consent to the processing of so-called "sensitive data" (e.g. health, religion, etc.), higher requirements may have to be set under certain circumstances in individual cases.

The new EU General Data Protection Regulation (applicable from 25 May 2018) for the first time creates clarity to some extent by establishing the minimum age of

consent at 16 years, but at the same time allowing the EU Member States the possibility of establishing a lower age limit (at least 13 years).

2.9 Period of the validity of the consent

It is regularly claimed that consent to the sending of email advertising expires after a certain period of time. However, there is no proof (even) in case law for such a limited "shelf life".

It should be ensured that the consent is used relatively promptly after it is given. In the opinion of the Munich I Regional Court with its judgment dated 8 April 2010, File Ref. 17 HK O 138/10, consent to the sending of email advertising which is not used more than 1.5 years later is no longer valid as the consenting party will no longer expect the email advertising to be sent after such a long period of time. If, however, consent is regularly given to the sending of an email newsletter, there is no reason to assume that it should expire after a certain period of time.

2.10 Demonstrability of the consent (double opt-in)

In the event of a dispute in court regarding the permissibility of sending advertising email, the sender has the burden of presentation and proof that the consent was actually given by the specific owner of the email address used. The mere presentation that consent to the sending of advertising emails to a particular email address was given is not sufficient if the sender cannot prove that the consent actually originated from the owner of the email address used.

As a fundamental rule, the sender must note the following:

- The mere granting of the addressee's consent is not sufficient. The consent must be obtained in such a way that it can be proven when convincing a court **(provability).**
- The consent from a person is not sufficient either on its own. It must be proven that precisely the recipient and not perhaps a third party using the recipient's name or email address has given consent **(congruence: registering party – (subsequent) recipient).**

For the proof that the consent actually originated from the owner of the email address used, the double opt-in procedure offers the maximum legal certainty. The use of the double opt-in process is therefore highly recommended – but it is not mandatory under the law. Let us repeat that: There is no statutory obligation to use the double opt-in process. Nor was such an obligation introduced with the 2009 amendment of the BDSG.

Why actually double opt-in?

As a reminder and for clarification: With the double opt-in procedure, a confirmation email (frequently also called an invitation email or a check email) is sent to the email address given during registration for a newsletter. In this confirmation email, the addressee is asked to confirm his or her consent by clicking on a confirmation link. If the addressee clicks on the confirmation link, it can thus be proven that the owner of

the email address which was given during registration actually submitted the consent.

By using the double opt-in procedure, it can thus be prevented that advertising emails are sent to an email address that has not been registered by its owner, but instead misused by a third party. It is also ensures that no advertising email addresses with which the user has merely committed a typing error during registration become a part of the distribution list. In this case, too, there is the risk that the actual holder of the email address receives advertising emails even though he or she never submitted consent.

And is the double opt-in procedure faultless from a legal perspective?

In the field of dialog marketing, contradictory court rulings can be found for virtually all legal issues. Unfortunately, the courts are and were also not entirely in agreement in the assessment of the double opt-in process. In some rulings, the confirmation email per se was already seen as an unreasonable harassment (or unlawful email advertising or spam). In the process, however, the courts have overlooked the fact that ultimately there is no alternative to the double opt-in procedure if you want to conduct legally sound email marketing. Not even in the (admittedly hypothetical) use of a Post-Ident procedure, or a notarized certification of the consent to the sending of email advertising, can it be established with legal certainty that, for instance, the email address angel23@gmx.com does indeed belong to Ms. Maier, who indicated precisely this address when giving her consent.

It was therefore a great step forward from a legal perspective that the German Federal Court of Justice in its judgment of February 10, 2011, File Ref. I ZR 164/09, which tellingly bears the title of "double opt-in process", basically gave a green light for the double opt-in process:

"If request for participation is received in electronic form, the sender of the request can be asked in an email to confirm his or her request to participate. After receipt of the requested confirmation, it can be assumed that the application did indeed originate from the email address indicated".

In contrast, the Munich Higher Regional Court ruled 27 September, 2012, that the confirmation email under the double opt-in procedure already constitutes an unsolicited advertising email. The confirmation email that is used precisely to avoid spam would therefore itself be spam according to the Munich judges.

In this manner, according to the Munich judgment, consent is required even for a confirmation email. However, as the confirmation email is used particularly to make the consent provable, there inevitably cannot be any provable consent for the sending of the confirmation email. Which means that you somewhat feel as if you were in a novel by Kafka:

"Do you want to obtain consent? But then please prove beforehand that you already have consent ...".

This would raise almost insoluble practical problems.

Under the following conditions, sending a confirmation email within the framework of a double opt-in process would be legal:

a) Confirmation email without advertising

The confirmation email must always be absolutely free of advertising and may solely be used to verify the email address.

As is seen frequently enough, the confirmation email does not have to be sent as plain text. It may indeed correspond to the corporate identity of the company and for instance include a logo, but additional advertising elements must be avoided. A confirmation email loaded with advertising would not be upheld in court and would be considered impermissible advertising email.

b) Confirmation email with full declaration of consent

The confirmation email serves solely to verify consent. If a user indicates a third-party email address in subscribing to a newsletter, either improperly or because he or she is of the opinion that the newsletter could perhaps interest the owner of the email address, the owner of the email address receives a confirmation email.

Without being familiar with the declaration submitted by the third party, the owner of the email address receives this confirmation email; he or she has never submitted any kind of consent on a website. If he or she now clicks on the confirmation link, this click alone must constitute sufficient consent in order to send the newsletter to his or her email address in the future.

The full consent should therefore be included in the confirmation email. And full consent must be given with the click on the confirmation link. Solely with the wording of the confirmation email, the sender must be able to prove in court that the addressee's consent to the sending of email advertising had been received. It is therefore not sufficient if there is a brief and concise request in the confirmation email for the confirmation of the consent submitted on the website during registration, without repeating it.

In other words: If you invest a lot of time and effort (and possibly even money for a legal audit) in the wording of your declaration of consent on the website, this declaration of consent must also be reproduced in exactly the same form in the confirmation email. Otherwise you can save yourself the effort.

c) Confirmation email without further explanations

The confirmation email should solely be used to confirm the consent and no further declarations should be packed into it. One of the numerous formal requirements for the validity of consent is that it is submitted separately from other declarations, in almost isolated form (cf. Chapter 2.2).

The confirmation of consent in the confirmation email should therefore, for instance, not be linked to participation in a contest.

Worst practice/negative example

One more click to big winnings! Please conclude your participation in our big million-dollar contest by clicking on the following link and confirming the conditions of participation in the contest and your subscription to our newsletter with current information.

In this case, there is no longer any separate declaration of consent and the consent would be invalid. The wording of the confirmation to be submitted must make clear that solely the consent to the sending of the newsletter is confirmed and not also the participation in the contest at the same time.

Best practice/positive example

Many thanks for your participation in our big million-dollar contest! Please confirm your subscription to our newsletter with up-to-date information. You can unsubscribe from this newsletter at any time with effect for the future, for example by sending an email to ...

What is the status of reminders when the addressee does not confirm immediately?

An (advertising-free) confirmation email is legally OK, but it may be the case from time to time that the confirmation email is overlooked or in the worst case perhaps caught in the spam filter. If the addressee does not click on the confirmation link, is it permissible to send a reminder email?

Unfortunately, there is no clear answer to this question. As stated above, it is indeed encouraging that the BGH established regarding confirmation emails that they do not constitute an unreasonable harassment. Regarding the question of whether a reminder email can be seen as an unreasonable harassment, the legislation has not been forthcoming to date, as far as we can tell. However, it is to be assumed that the courts will view such a reminder email significantly more critically than the confirmation email per se. The confirmation email serves solely the purpose of verifying the email address and thus acquiring a more legally sound and flawless consent. However, the reminder email tends to serve the purpose of indicating a confirmation that has not been given and to perhaps gain consent after all, even if the addressee has not confirmed it in the first run, for whatever reasons. It may therefore become more difficult here to substantiate legitimate interest beyond the growth of the distribution list in the sending of the reminder email. By this, however, the aim is not to state that the sending of such a confirmation email is clearly impermissible.

If a reminder email is sent, however, it should generally only be sent once and within a relatively short period after the sending of the confirmation email. Regular reminder emails over a period of several weeks or months will, with reasonable certainty, annoy the addressee and lead to complaints.

Deletion of the data in the event of non-responders

How long can the data be stored then if there is no confirmation? Here, too, it is difficult to indicate an absolute period of

time. In abstract terms, it can be stated that data may only be saved for as long as they are required to carry out the double opt-in procedure.

Thus, we arrive at the question of how long such an appropriate period of time is, i.e. how long the confirmation from the addressee can realistically be anticipated. Based on experience, the ordering of a newsletter is confirmed within a few minutes. If, for instance, the addressee is on holiday and is not lucky enough to be reachable via email, however, it may indeed take one or two weeks until the addressee confirms his or her subscription to the newsletter. Accordingly, a period of two weeks is still seen as permissible under data protection law.

Tell-a-Friend function

With the so-called Tell-a-Friend function, internet users can inform their friends about an Internet page visited. They just type in the email addresses of their friends in a form directly on the web page and the friends will receive an automated email with the respective URL. It is debatable whether the emails sent in this manner are considered impermissible email advertising by the provider of the Tell-a-Friend function, or permitted private messages sent by the user of the Tell-a-Friend function to his friends.

With the judgment of 12 September, 2013, File Ref. I ZR 208/12, the BGH considerably reduced the use of such Tell-a-Friend functions and subjected them to certain requirements. The following facts were available to the BGH: The plaintiff received product recommendations several times without his prior consent from the defendant who had set up a "Tell-a-Friend" function on its website. In the process, the defendant was (also) named as the sender of the recommendation email. The plaintiff therefore wanted to file a claim for injunctive relief against the defendant. The courts of prior instances (Cologne Local Court and Regional Court) had rejected such a claim on the grounds that the defendant would not be liable for the misuse by a third party with regard to the "Tell-a-Friend" function.

However, the BGH did not share this opinion: Initially, the BGH qualified the disputed recommendation emails as advertising pursuant to the Directive 2006/113/EC (accordingly, any statement when carrying out commerce, trade, craft or free profession with the goal of promoting the sale of goods or the provision of services is defined as advertising activity – see Point 2.2 above for the definition of advertising). In addition, recommendation emails are always to be assigned to the sphere of the website operator, irrespective of whether a third party initiates these emails. An important factor in particular is that the defendant appears as the sender in relation to the recipient of a recommendation email. Ultimately, it is also the meaning and purpose of the "Tell-a-Friend" function to draw attention to the website and the services offered there. It is thus stated in the grounds for the ruling:

"This assessment is not countered by the fact that the Defendant does not tolerate the misuse of the "Tell-a-Friend" function. It is apparent that the "Tell-a-Friend" function is used precisely to send recommendation emails to third parties, without there being

any certainty that they have given their consent in this respect".

Consequently, when the recommended company appears as the sender, a decisive factor in the Tell-a-Friend function is then at least whether the recipient has given his or her express consent to the unsolicited sending of such content. If no consent has been given, the protection of the consumer is required who is powerless against the sending of unsolicited advertising emails. In these cases, the emails are impermissible pursuant to Section 7 para. 2 no. 3 UWG.

The Superior Court of Justice in Berlin in its judgment of 24 January, 2014, File Ref. 5 U 42/12 implied that the Tell-a-Friend function can be made available legally under certain conditions. A crucial prerequisite is that the message must be sent to the addressee as a private message from a friend, who initiated the dispatch, and not sent as a commercial communication by the provider of the Tell-a-Friend function. The above-mentioned case was about the "Find a Friend" function of Facebook. In this case emails were sent in the name of a Facebook user's email address to all email addresses in the address book of the Facebook user, inviting contacts who are not yet Facebook members to use Facebook. Unlike the above-mentioned judgment of the BGH dated 12 September, 2013, the Facebook user was named as the sender, and not the advertised company. The Superior Court of Justice in Berlin took the view that this is not considered email advertising by the advertised company if the latter only provides technical assistance for the dispatch. In the opinion of the Court, emails sent by using the Tell-a-Friend function are attributable to the user if the latter initiated the dispatch of the email at their own initiative and with full knowledge of all the circumstances of the dispatch. In the case decided by the Superior Court of Justice in Berlin, precisely this full knowledge of all circumstances was missing. Facebook had not clearly informed the user that emails would be sent in their name to all email addresses contained in their email address book and belonging to individuals who are not yet Facebook members. Due to this lack of transparency in the design of the Tell-a-Friend function, the court considered Facebook as responsible for the dispatch of the emails. The BGH confirmed the judgment (judgment from 14 January, 2016, File Ref. I ZR 65/14), however, the grounds for the decision are not currently available, so that it is not clear whether the court dealt any further with the issue of the fundamental admissibility of the Tell-a-Friend function.

2.11 Documentation of the consent

Irrespective of the procedure used, the declaration of consent must be documented comprehensively and permanently for the entire usage of the email address, whereby the documentation requirements of the BGH (judgment dated 10 February, 2011, I ZR/164/09) are to be taken into account in the recording process. In the case of dispute, the sender of an advertising email must be able to at least present the following details:

- Content of the declaration of consent and information about the form (how was the consent declared: actively and separately?)
- Time of the declaration of the consent
- IP address of the consenting party at the time the consent was given (with dynamic IP addresses, the IP address of course only has a very limited value as proof)

- If applicable, the time when the invitation email was sent out (with double opt-in)
- Content of the invitation email (with double opt-in)
- Time of the confirmation of the consent (with double opt-in)

In the case of a consent granted through personal contact, it may be possible under certain circumstances to use the recipient of the declaration as a witness, apart from the written confirmation. In the event of a dispute (in court), the recipient's statement must be considered credible. There are doubts in this regard if the contact took place a considerable time ago and was made within the framework of many other contacts, for instance at a trade fair. In addition, it is also not ensured that the contact person is actually the person who receives the advertising later on. Here, too, the carrying out of an - accordingly adapted - double opt-in procedure lends itself.

2.12 Exception from the opt-in: Email advertising with existing customer relationship

For email advertising within the framework of existing customer relationships, the law makes provision for an alleviation in Section 7 para. 3 UWG. Normally, the advertising company requires the conscious and unequivocal consent from the addressee in order to be able to send advertising emails (so-called opt-in). With an existing customer relationship, however, the customer may be sent advertising emails if the customer has not objected to them being sent (so-called opt-out). This exception to the rule, however, has certain formal requirements, which is why it is also called a "qualified opt-out"[1]. Specifically, these requirements are as follows:
The sender must have received the customer's email address "in connection with the sale of goods or services".

In addition, it must have been pointed out to the customer "in a clear and unequivocal manner in the collection of the address and in each use thereof" that he or she can object to the use of his or her email address for advertising at any time, "without costs other than the transmission costs pursuant to the basic rates being incurred in this regard" – and of course the customer must not have objected to it.

In the emails subsequently sent to the customer, solely "the company's own similar goods or services" may be advertised.
The law clearly states that the customer must give his or her email address him- or herself to the advertiser during the order process. Accordingly, it is not sufficient if the advertiser has received or found out the customer's email address by other means.
A hotly debated issue is the question of whether the sales process must actually be completed to be able to use the email address for email advertising. This question becomes relevant, for instance, with inquiries from prospective customers and in the online shop with so-called shop drop-outs who, in the course of the order process, place merchandise in the shopping cart and indicate their email address but then cancel the order process. In such cases, are the statutory requirements "in conjunction with

1 As already explained, the opt-in process is basically always applicable in Germany. Only if the strict requirements of Section 7 III are met, this is exceptionally known as a so-called (qualified) opt-out or a soft opt-in.

the sale" already met or must the sale be definitively completed?

While it is undisputed in many other European countries that contract negotiations are sufficient for reference to the exception to the rule, there is much disagreement in this regard in Germany. On the one side, there are the advocates of the most far-reaching protection against annoying email advertising, who propagate a narrow interpretation of the exception to the rule and see the conclusion of the sales process as a mandatory requirement. An argument in favor of this is also the wording of Section 7 para. 3 UWG that expressly mentions CUSTOMER. On the other hand, it is stated that a prospective customer who has voluntarily given his or her email address during an order process and has been informed that he or she will receive email advertising in the future if he or she does not object, is not particularly worthy of protection.

In using email addresses that were collected "in conjunction with the sale of goods or a service," there is thus a residual risk if this sale is not definitively concluded. There is no definitive court ruling that provides an unequivocal answer to this question (as far as is discernible).

In order to apply the exception to the rule given in Article 7 para. 3 UWG, it must be a payment-based legal transaction. In the case of a free of charge service, for instance a free membership in an internet platform, the prerequisites of Section 7 para. 3 UWG are not fulfilled.

At any rate, a forwarding of the email address to other companies, even to group companies, is not permissible. Usage of the address for advertising purposes for other companies is not permissible either.

In addition, the advertising company may only send the customer email advertising for "its own similar goods or services". Here, the question arises with regard to what is meant by this abstract wording. The required similarity between the goods purchased and the goods that may be subsequently advertised is determined from the customer's perspective. Based on the purchases up to that point, the advertiser must ask itself the question as to what other similar goods the customer might possibly be interested in.

According to case law, the decisive factor for the similarity of the goods is whether the advertised goods correspond to the same typical intended use or customer need as those related to the products that the customer already purchased. If both goods are used for the same typical intended use, the similarity is given. In the process, accessories and supplementary goods are still recognized by the case law as "similar", even if the case law fundamentally assumes a narrow interpretation of the exceptional circumstances.

If a customer, for instance, orders French red wine, he or she will undoubtedly also be interested in wines from Austria or other countries – it is therefore permissible to inform him or her about them. The information about accessories for the goods originally purchased should also easily fall under the exception to the rule. Specialized

online dealers who only offer goods from a certain segment will therefore be able to use the exception to the rule better than an mail order company with an extensive range of goods who advertises goods in its newsletter from all areas in an unspecified form.

If the advertiser has used an "active opt-in" up to now within the framework of its online shop in which the customer must click on a check box in order to receive its newsletter in the future, it can, as an exception, integrate this check box in "pre-clicked" form in the order process, in the case of sending advertising for its own similar products within the framework of the above-mentioned customer relationships. In the process, it must always be pointed out that the sending of advertising emails can be objected to at any time, without costs other than the transmission costs pursuant to the basic rates being incurred in this regard.

The user must become active in this case and "disable" the check box if he or she does not want to receive advertising emails on their own similar products. Experience shows that such a changeover results in at least a doubling of the conversion. The advertiser must then, however, of course note the restriction of the advertising to "own similar goods or services". If he or she wants to use the addresses acquired in this way for the sending of the newsletter, he or she may only advertise goods of a similar type.

For example, a travel operator who integrates the following text in its order process should generate considerably higher conversion:

We will send your booking confirmation to the email address indicated. In connection with your booking, you will receive from us, in addition to the booking confirmation, other emails with information and offerings tailored to your trip. You can object to the sending of these emails at any time by sending an email to unsubscribe@xyz.com, without costs other than the transmission costs pursuant to the basic rates being incurred in this regard. After receipt of your objection, we will suspend the sending of emails immediately.

This form guarantees a virtually 100% conversion; however, the content of the subsequent advertising communication should definitely be restricted to information that is actually limited to the specifically booked trip. It is also important to note that only "own" products may be advertised.

Information about the right of objection must be provided directly when the email address is collected, i.e. at the point in time when the customer notifies the advertiser of his/her email address. Existing customers who did not have their right of objection pointed out to them when they indicated their email address cannot have this pointed out to them subsequently by email. Rather, they must be motivated to provide their email address again and then have their right of objection pointed out to them. For this purpose, the customer can, for instance, be subsequently offered an additional service (possibly also for free), during the order of which the email address is then to be given. However, the subsequent qualification is made more difficult by the fact that existing customers may not have the additional service pointed out to them

by email. Here, alternative forms of contact, for instance via the website, by mail or as part of transaction emails are to be selected.

2.13 Advertising in transaction emails

Transaction emails are emails that a company sends as part of the fulfillment of a contract, for instance, order confirmations, dispatch confirmations or invoices. For such transaction emails, the sender does not, of course, require the consent of the addressee. From a marketing perspective, it lends itself to also advertise for other products and services of the sender in such transaction emails, as advertising in transaction emails has above-average conversion rates.

The major question here is: May transaction emails contain advertising if the addressee has not consented to the sending of advertising emails and if the requirements of the exception for email marketing with existing customer relationships (cf. 2.12) are also not met?

For advertising emails, the addressee's consent is required as an "unreasonable harassment" through unsolicited mass advertising is to be avoided. In the legislator's opinion, the "unreasonable harassment" lies in the addressee being forced to deal with every email that he or she has received and to delete it if it is unsolicited advertising. However, this "unreasonable harassment" cannot exist at all with a transaction email. The addressee receives the transaction email, i.e. for example the dispatch confirmation, at any rate and has to handle it, irrespective of whether this also contains advertising content as an accompanying measure or not. It is a different case, however, when advertising is hidden in the transaction emails, even if it only appears as an accompanying measure. No later than when the addressee has expressly objected to advertising being sent, the sending of advertising in permissible transaction emails is illegal in any case. In this context, the BGH in its judgment of 15 December, 2015, File Ref. VI ZR 134/15, decided that advertising in an auto-reply email, for example, the automated acknowledgement of receipt of an email is illegal if previously the addressee had expressly objected to the sending of email advertising. In this specific case, the plaintiff terminated the contract with the defendant insurance company by email. He then received an automated acknowledgement of receipt by email which contained a short mention of a severe weather warning service belonging to the insurance company at the end. The plaintiff then replied by email to the insurance company and expressly stated that he objected to the advertising contained in the automated acknowledgement of receipt that was sent. A week later in response to this email, and to another email requesting information on the status, he again received an automated acknowledgment of receipt referring to the severe weather warning service.
The BGH ruled that at least the last confirmation email received from the insurance company was illegal.[2]

2 Brief explanation: The BGH took into account the basis for claim in Sections 1004 and 823 BGB (Bürgerliches Gesetzbuch [German Civil Code]), since the plaintiff as a private subject had no claim pursuant to the UWG. The Court states in its judgment that any advertising without consent constitutes an unreasonable harassment (UWG). Unfortunately, the BGH leaves the question open regarding the extent to which an infringement pursuant to Art. 13 EU-DS_RiLi, referred to in the judgment within the context of Section 823 BGB, is relevant. However, this should not lead to the conclusion that advertising in transaction e-mails until objection is acceptable.

On the one hand, in the opinion of the BGH, the reference to the severe weather warning service is advertising (see above under Point 2.2 for the definition of advertising). And on the other hand, the advertising was sent against the express declared will of the addressee - and was thus an unreasonable harassment of the addressee.

2.14 Feedback inquiries after purchase

Customer feedback is extremely valuable for many companies to enable them to improve the products and services they offer and to adapt them to the requirements of the market. In addition, customer ratings are increasingly becoming the basis for purchase decisions. More and more suppliers are therefore sending emails out after a purchase has been made, with the request for a rating and feedback from the customer.

However, are such feedback inquiries also permissible after purchase if the addressee has not consented to the sending of advertising emails and if the requirements for exemption from email marketing with existing customer relationships (cf. above) are also not met?

The decisive question here is whether feedback inquiries are advertising. The Coburg Regional Court answered in the negative (judgment dated 17 February, 2012 File Ref. 33 S 87/11). Accordingly, a one-off feedback inquiry is not advertising but primarily "customer service that aims to help improve processes and eliminate defects". Furthermore, feedback inquiries have since then also become common practice. The court therefore did not see consent by the addressee to advertising as being necessary. This ruling was strongly criticized, in part with good arguments. It is also not certain under any circumstances that other courts would decide exactly the same when it comes down to it. You are therefore on the legally permissible side if you meet the formal requirements of the exception in email marketing with existing customer relationships (cf. above).

2.15 Legal consequences in the case of non-compliance with statutory requirements

In the event of a dispute in court regarding the permissibility of the sending of the advertising email, the sender has the burden of presentation and proof within the meaning of Section 13 para. 2 TMG, Section 7 para. 2 no. 3 UWG, Section 28 para. 3a BDSG that the consent was actually given by the specific owner of the email address used. The mere explanation that consent to the sending of advertising emails to a particular email address was given is not sufficient if the sender cannot prove that the consent actually originated from the owner of the email address used. The minimum requirements are the text of the consent at the time of the data collection, date and time, and consent source (see Chapter 2.11.)

At present, more and more recipients are protesting against unsolicited commercial emails. In the year 2015, the eco Complaints Office recorded more than 190,000 email-related user complaints.

Legal disputes that have as their object the legality of sending advertising emails are not

very common because the parties usually try to settle outside of court. Out-of-court procedures also have costs, but compared to a legal procedure these are still manageable. This includes e.g. warning costs and legal fees, as well as claims for compensation for damages.

If the matter escalates to legal proceedings, the sender of advertising emails can expect high costs in the event of losing the case: The costs of the legal proceedings are calculated according to the corresponding amount in dispute by the competent judge. The amount in dispute can be from EUR 100 to over EUR 30,000 (BGH I ZR 38/10) and may vary depending on the individual case and judicial instance. In the event of a dispute value of EUR 30,000, the sender could face attorney's fees, court costs as well as a compensation for a total amount of over EUR 5,000. If, for example, four recipients of unsolicited commercial emails take legal action against the sender, he or she could face costs up to EUR 20,000. In addition, mailers of illegal advertising emails could be ordered to refrain from the illegal action. In this case, the courts also threaten to impose a fine to the amount of up to EUR 250,000 for each case of infringement, provided this has been requested by the plaintiff.

It is therefore recommended that all conditions for a legitimate dispatch of advertising emails should be observed in order to avoid any high legal costs and claims to compensation for damages.

3. Unsubscribing

3.1 Can one easily unsubscribe from emails?

Those who send advertising emails are obligated to give the recipients the opportunity to delete their names from the distribution list and to clearly point out this possibility (Section 28 para. 4 BDSG, Section 7 para. 2 no. 4 UWG, Section 13 para. 2 no. 4 TMG, Section 13 para. 3 TMG). The best variant is an unsubscribe link directly in the email. After clicking on this link, the deletion must be carried out in a prompt manner.

The information with regard to the unsubscribe option must already be available when consent is obtained.

The legislator stipulates that the service provider gives the users the option of revoking their consent to the use of their data and/or opt-in at any time (Section 13 TMG and Section 28 para. 4 BDSG). In addition, the legislator expressly demands that the information regarding this right must be given to the user as a mandatory measure before the declaration of the consent (Art. 13 para. 3 TMG)

It is therefore not sufficient to place the information in a newsletter with an unsubscribe link. The legislator already demands corresponding information during registration.

Ostensibly, this formality appears unimportant and rather self-evident. Particularly since, with this notice, users are also alleviated of some of their fear to give their consent "forever". Nevertheless, not all

companies by far succeed in meeting this requirement of the legislator.

Because such information also generates trust, this opportunity should be used and the recipients given the assurance that they can unsubscribe to the newsletter at any time (with just one mouse click).

Wording examples:

- You can easily unsubscribe to the newsletter at any time with effect for the future with just one click of the mouse.
- In every newsletter, we will offer you the possibility of terminating your subscription.
- Each newsletter will contain an unsubscribe link via which you can independently unregister at any time with one click of the mouse.
- You can object to the use of your data for advertising purposes at any time.

The implementation of the objection to the further processing or usage of the contact data of a person in question for advertising purposes must be done immediately in the respective company, Section 28 para. 4 sent. 1 BDSG.

The unsubscribe option must be given in each advertising email.

It is stipulated by law that an unsubscribe option must be made available in each advertising email and reference must be made to it (Section 7 para. 2 no. 4 UWG, Section 7 para. 3 UWG, Section 13 para. 2 no. 4 TMG and Section 28 para. 4 BDSG):

If the person in question files an objection to the responsible organization regarding the processing or usage of his or her data for purposes of advertising or market or opinion research, processing or usage for these purposes is not permissible. When approached for advertising purposes, the person in question must be informed [...] about the organization responsible and about the right of objection [...];

This means that: The (subsequent) recipient must have his or her right of objection pointed out to him/her. As soon as they announce that they would not like to receive any further emails from the sending company, it must be ensured that they are promptly excluded from future mailings. The opposition to an objection pursuant to Section 28 para. 4 BDSG can be punished with a fine of up to EUR 300,000 (Section 43 para. 2 no. 5b BDSG, Section 43 para. 3 BDSG.

There are several ways to point out the right of objection to the recipients. But they are not all to be recommended.

The best way and most user-friendly is the integration of an unsubscribe link in each email sent. This link is generally at the end of the email.

An example:

If you no longer want to receive our newsletter, simply click here: Unsubscribe to newsletter

Professional email marketing systems ensure that any user who clicks on this link will automatically not receive any more emails.

After clicking on the link, the user should land on a page on which the deletion from the distribution list is confirmed.

Wording examples:
We have deleted you from our distribution list. You will not receive any further emails from us.

It is not necessary to confirm the unsubscribe request to the user by email. In fact, this additional email can be understood by the users as an unreasonable harassment as they have just withdrawn their consent to the advertising company sending them any more emails.

No processes should be used that make it more difficult for the user to unsubscribe, such as the so-called "double opt-out" in which the user receives an email after unsubscribing and is requested to confirm the unsubscribe by clicking on a link.

Experience shows that a not-to-be-underestimated percentage of users does not click on this link: Perhaps precisely this email got caught in the spam filter by mistake, or the user thought the email was nothing but a confirmation of the unsubscribe, without reading it in more detail – there are many possible reasons. The fact is that in this case the user will continue to receive the respective newsletter. This often leads to the user getting annoyed quickly – which is not really what the newsletter actually wanted to achieve.

Some email marketing systems do not offer the use of automatic unsubscribe links. The unsubscribe is implemented by email in this case. There are two common variants.

Example variant 1:
To unsubscribe to our newsletter, reply to this email and write "unsubscribe" in the subject line.

Example variant 2:
If you do not want to receive any other emails from us, please send an empty email to unsubscribe-635094235835@companyname.com.

In both cases the email marketing system monitors the incoming mails and removes the recipient from the distribution list.

Unsubscribes by email are also used for the so-called "list unsubscribe". Unfortunately, this is not yet standard and thus only a few email programs and web mailers currently offer their users this additional service. The way it works is pretty straightforward. The sender not only integrates the unsubscribe link in the content of its newsletter, but also stores it in the email header. The email program or the web mailer then provides an extra button for unsubscribing. If the recipient clicks on it, an email is automatically sent in the background to an email address provided by the sender for this purpose and the newsletter is unsubscribed. Advantage of this variant: The "unsubscribe" button has a fixed place in the email program and applies to newsletters of all senders who support the "list unsubscribe" method. A search for the unsubscribe link in the newsletter is thus no longer necessary.

In addition, there must be the possibility of also correctly processing unsubscribes via other means. If a user therefore sends an informal email in which he or she asks to be deleted from the distribution list, it should be guaranteed that this inquiry is read and processed promptly.

Companies who are in contact with their customers via a call centre or hotline must ensure that unsubscribes that are received over the phone are processed promptly and are not simply "lost".

The variant of also offering an unsubscribe form on the website and in which the user enters his or her email address, in addition to the subscribe form, is not recommended (or is at best suitable as additional measure). Reason: Many users have their emails redirected from one email account to another and in cases of doubt, no longer know which of their various email addresses they used to subscribe. Some users will therefore be unable to unsubscribe, which harbors potential for frustration.

However, it could be even worse.

Worst practice/negative example

In order to unsubscribe to the xyz newsletter, please log in with your user name and password under www.xyz.com. Then access the area "My profile" and remove the tick next to "Newsletter" in the section "Email settings".

Such a procedure is firstly complicated and secondly there is a high probability that a not-to-be-underestimated percentage of the users have already long forgotten their original registration data.

Checklist

- ✔ Was the unsubscribe option pointed out when consent was given?
  ☐ Yes ☐ No
- ✔ Is reference made on all online and offline forms to the unsubscribe option?
  ☐ Yes ☐ No
- ✔ Does each commercial email sent contain an unsubscribe option?
  ☐ Yes ☐ No
- ✔ Is the unsubscribe directly possible (without double opt-out or mandatory login)?
  ☐ Yes ☐ No
- ✔ Is the address deleted promptly from the distribution list after unsubscribing?
  ☐ Yes ☐ No
- ✔ Is it ensured that cancellations received via other channels are also handled promptly?
  ☐ Yes ☐ No

3.2 Are inquiries and complaints responded to?

Email advertising is dialog marketing. It is, therefore, particularly important that inquiries and complaints are answered quickly. Particularly because email marketing is such a fast medium, companies should not allow themselves any negligence here. Twenty-four hours are usual.

People who make complaints or give feedback fundamentally have a great interest in the company:

- When complaints are recorded and processed properly, they can even be turned into their opposite (goal: satisfied customer).
- Feedback of any kind also always helps an improvement process – what is done well at the company, what is not done well?
- Feedback can pave the way for specific business: Particularly with emails, many people are used to simply pressing "Reply". A company should not waste this opportunity for dialog.

Responses to emailings are received by a company via several channels:

1. Every email dispatch has bounce mails - holiday messages and other auto-replies (e.g. "I have changed the department, the person responsible is now Mr. Müller»), undeliverable messages, acknowledgments of receipts, "genuine" responses, etc.
2. "Genuine" email responses that are received via the published support email address.
3. Responses by other means, such as telephone, fax, letter, or lawyer.

Virtually all modern email marketing systems filter holiday announcements, bounces, etc. out automatically and process these emails further (e.g. bounces are blocked from further mailings). The challenge in this case is to filter "genuine" responses. This can be done manually or automatically. Under no circumstances may the content of the mailbox be simply deleted for the "reply to" address.

The "genuine" responses filtered in this way can now be processed in exactly the same way as the responses that are received via the normal support email addresses.

Text components that provide answers to the usual standard questions are recommended. In order to make the processes of answering several tens of thousands of emails manageable in a short period of time, there are special response management systems. It is a "matter of conviction" whether to give preference to fully automatic systems with "artificial intelligence" or more to "rule-based systems" that support the call center agents, but do not replace them. As a rule, customers tend to react testily when they receive a response that has (apparently) been generated automatically. The more specifically the subject of the question is addressed, the more likely the customer is to be satisfied.

The recipients rarely ring. It is crucial that the call center agents have access to the email database so as to at least be able to definitively answer the most important questions ("Where did you get my address from?", "Please do not send me any further emails!").

In both cases (the electronic feedback and the feedback by other means), it is crucial that the processes for responses and complaints are defined and documented. The speed of the response is of particular importance – with the fast medium of email, the expectation is a response within 24 hours.

Checklist:

- ✔ Is a support address given in the email which can be contacted by email or by telephone?
  ☐ Yes ☐ No
- ✔ Is it ensured that the sender/"reply to" address works and that messages addressed to it do not land in "cyberspace"?
  ☐ Yes ☐ No
- ✔ Are email returns to the sender's address automatically filtered and adjusted to reflect bounces / holiday notifications?

☐ Yes ☐ No

✔ Are "genuine" email returns reviewed and either answered directly or forwarded to the corresponding departments on a continuous basis by an AI system or an employee?

☐ Yes ☐ No

✔ Does the call center have access to the email database, e.g. to be able to carry out immediate blocking of addresses?

☐ Yes ☐ No

✔ Is the call center informed about the outgoing emails?

☐ Yes ☐ No

✔ Are there checklists and procedures on how "critical" cases are to be handled?

☐ Yes ☐ No

✔ Are there analyses of response time and quality / satisfaction with response?

☐ Yes ☐ No

✔ Are requests / complaints answered promptly (twenty-four hours are usual)?

☐ Yes ☐ No

4. Design of newsletters

Some legal requirements must also be observed in the design of the newsletter itself.

4.1 Subject

Commercial communication by email must always be clearly recognizable as such (Section 6 para. 2 TMG). The subject of the newsletter should not conceal the fact that it is an email for advertising purposes. Such a concealment is when the sender of the email designs the subject intentionally to mislead recipient about the commercial character of the email.

The explanatory memorandum includes the following examples of deceptive subject lines:

- "Final Warning"
- "Caution, extremely urgent!"
- "Your criminal proceedings File. Ref. XY"

Such subject lines supposedly ensure that as many recipients as possible open the email. However, the recipients must be protected from having to open advertising emails to determine whether the email contains relevant content. Moreover, on the basis of the subject, recipients should be able to recognize that it is an advertising newsletter.

However, that does not mean that the term "Newsletter" must be necessarily mentioned in the subject line. The commercial nature of an advertising email can also be identified in other promotional-typical wordings.

Examples:

- "Your Offer of the Week"
- "Only until Sunday – 20% discount on the whole product range"
- "Go spring shopping cheap now"

From a marketing standpoint, the subject of the newsletter should be as brief, precise and appealing as possible. A personal greeting in the subject of the newsletter can speak to the newsletter recipients on more of an individual level.

In addition, with email marketing it should be taken into consideration that the subject line of the email is checked by means of spam filters. Therefore, all terms and phrases should be avoided which can lead to the newsletter landing in the SPAM folder.

Examples:
- Special characters (e.g. $!?)
- CONSISTENT CAPITAL LETTERS
- Free-of-charge, free, guarantee
- Order today! Order now!
- Money-back guarantee
- Poker, casino, chance to win

SPAM filters change constantly in order to catch up-to-date SPAM waves. In case of doubt, newsletter mailers should therefore check whether their newsletter may have to be fished out of the normal SPAM filters. There are providers with whom you can check for free if the newsletter is being identified as SPAM.

4.2 Content

With respect to the content of the newsletter, the commercial background must be clearly identifiable as such (Section 6 para. 1 no. 1 TMG). The sender must also be identifiable (more under 4.3). If the newsletter contains special promotional offers (such as discounts, premiums and gifts), the conditions which are to be met to qualify for them must be easily accessible and presented clearly and unambiguously (Section 6 para. 1 no. 3 TMG).

Example:
The online shop XY offers a temporary discount campaign. It promotes this campaign in the newsletter under the title *"Super Summer Sale at XY – now an extra 20% off all reduced items".*

In this case, the customer must be informed of the conditions of the discount, whether it is temporarily limited and if a minimum order value is applicable. The customer must also be informed on the exclusion of individual brands or products. Ideally, this information should be made available at the end of the email and must be connected by an asterisk note with the eye-catching offer. Alternatively, the supplementary notes can be made accessible by a clearly visible link. In the above example the note could look as follows: *"Valid from 15-31.08.2016, applies only to discounted items, minimum order value of €50, brands A&B are excluded from the offer".*

The advertising nature of prizes and games must be clearly identifiable as such and the conditions of participation must be easily accessible and presented clearly and unambiguously (Section 6 para. 1 no. 4 TMG).

Moreover, a newsletter must comply with all requirements of other laws. A newsletter is a business action, such that the provisions of the Law against Unfair Competition (UWG) must specifically be observed.

In accordance, advertising statements may not be misleading (Section 5 UWG) or influence the consumer in an impermissible manner (Section 4a UWG). In addition, advertising may not be disguised as information or editorial content (no 11 of the Annex to Section 3 para. 2 UWG). If a competitor is discernible in the advertisement, the provisions on comparative advertising (Section 6 UWG) must be observed. Email advertising must therefore always meet the same requirements as advertising distributed via other channels.

If prices are specified in the newsletter, it is important to ensure that the provisions of the PangV (Preisangabenverordnung

[German Price Indication Ordinance]) are met. This means, for example, that every price indication to end users must indicate that the sales tax is included in the price. Any additional costs such as shipping costs, must also be clearly indicated. In the case of certain products a basic price must also be specified (Section 2 PangV).

If any copyright-protected content is used in the newsletter, make sure that the necessary usage rights have been obtained. This applies both to photos or graphics, as well as text.

Checklist Content:

- ✔ The commercial background must be clearly identifiable.
- ✔ In the case of discounts, premiums and gifts, the conditions must be easily accessible and presented clearly and unambiguously.
- ✔ In the case of prizes and games, the conditions of participation must be easily accessible and presented clearly and unambiguously.
- ✔ Advertising statements must not be unfair, e.g. misleading
- ✔ Price details must comply with the legal requirements, e.g. sales taxes, shipping costs, basic price information
- ✔ Licenses to copyright-protected content must have been purchased

4.3 Identification of the sender

The law prescribes that the sender of the newsletter must be clearly identifiable (Section 6 para. 1 no. 2 TMG). This does not mean the actual sender, but the advertisers, on whose behalf the newsletter is sent. So it is not the employee Mr. X, who is responsible for the dispatch of newsletters, who must be identifiable, but the company on whose behalf Mr. X. sends the newsletter. It is not permissible to disguise or conceal the sender of the email (Section 6 para. 2 TMG). The legal justification cites here as an example that the sender data suggests that the email is coming from an official body, e.g. an authority. It is also unacceptable to not mention any sender. The recipient must know who has sent the email.

When selecting the sender address, care should be taken to ensure that this gives a trustworthy impression. A clearly allocated address such as newsletter@company.de is suitable. SPAM filters should also be considered here. These often filter out questionable sender addresses automatically.

4.4 Legally sound legal notice

A Legal Notice is required on Internet pages. The law establishes a legal obligation for "commercially" offered internet pages (Section 5 TMG), as well as for Internet pages with journalistic and editorial content (Section 55 RStV (Rundfunkstaatsvertrag [German Interstate Broadcasting Treaty])). Therefore, in principle, all Internet pages require a Legal Notice, not solely for private purposes.

The same principles also apply to advertising emails/newsletters.

What compulsory information is there?
The law regulates the mandatory information that must be included in a legal notice:

- › Name of supplier, and in the case of companies: Corporate name and legal form

- Authorized representatives (in the case of legal entities)
- Postal address at which the sender can be summoned (so not a P.O. box)
- Email address
- Telephone and fax number, if applicable
- If available, commercial, cooperative, association, or partnership register number
- If available, VAT identification number and/or business identification number
- In the case of journalistic and editorial content: Name of the publisher *(responsible party pursuant to press law)* or person responsible for the content and, with legal entities, that of the authorized representative

Moreover, in individual cases further information may be required, e. g. professional legal information for physicians, pharmacists, lawyers or tax consultants.

In addition, mandatory details under commercial and corporate law must also be taken into account. Whether and which information is necessary is determined according to commercial and corporate law. For joint stock corporations (AG), for instance, other mandatory information applies as for the sole proprietor or the limited liability company (GmbH).

Template Legal Notice for a limited liability company

Anycompany Ltd
Represented by the managing director John Anyman
1 Any Street
Anytown, AB 12345

Email: sample@sample.com
Phone: 0123-45 67 89
Fax: 0123-65 43 21

VAT ID: DE 123456789
Sample Local Court, HRB 1234

How should the legal notice be integrated?

The legislator requires that mandatory details must be

- easily discernible,
- directly accessible, and
- permanently available.

The legal notice should therefore be referred to as such and be easily found without a long search. The font size should be selected so that the text is clearly legible.

The mandatory details do not necessarily need be in the email itself. A link to the legal notice in the homepage can also be placed in the email. Case law has acknowledged that a legal notice which is accessible by a maximum of two clicks meets the statutory requirements.

5. Profiling and evaluation of the opening and clicking behavior

Email marketing can be optimized by analyzing the interests of potential customers. Marketing can be refined using personalization or individualization. Personalization can be performed by evaluating the opening and clicking behavior of the email recipients, evaluating the otherwise acquired interests of the persons in question or through a combination of various possibilities. The main legal standard for the admissibility of this action is data protection law.

5.1 Application of data protection laws

Data protection law must be observed if personal data is collected or used (Section 1 para. 2 BDSG). This includes all information relating to an identified or identifiable natural person. Therefore, it is crucial that the data collected and used can be attributed to a specific or determinable natural person.

What is required for such a determination and thus for the application of data protection law is controversial in the legal world. Simply put, the discussion is as follows: In accordance with the **so-called subjective approach,** it is crucial whether the place that has the data can itself make the connection to a person. This view is mainly supported in the legal literature and in the case law from the highest courts. On the other hand, the **so-called objective approach** takes into account whether this is possible or not given the possibility of external third parties. The German data protection supervisory authorities tends to agree with the latter view. Due to the different interpretation by the courts and the supervisory authorities, the practical relevance of this uncertainty is evident.[3] In this case, the BGH also tends towards the subjective approach. The BGH has submitted the matter to the European Court of Justice (ECJ) for a decision.[4] This is because the decision must be made based on the interpretation of European data protection law (Data Protection Directive 95/46/EC). A decision of the ECJ is expected in 2016.[5]

However, there is consensus that data protection law is not applicable to **anonymous data or anonymized data.** According to the legal definition given in Section 3 para. 6 BDSG, anonymization means the modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labor be attributed to an identified or identifiable individual. It is obvious that the question as to when this is given is in connection with the interpretation of the ability to identify a person. Anonymization must be distinguished from pseudonymization. In accordance with the legal definition given in Section 3 para. 6 BDSG, "pseuydonymization" means replacing a person's name and other identifying characteristics with a label, in order to preclude identification of the data subject or to render such identification substantially difficult.

The crucial difference is: Data protection law is not relevant to the collection and use of anonymous data. In the collection and use of pseudonymized data, data protection law must be fully observed. However, data protection law sometimes simplifies the use of pseudonymized data (see below on Section 15 para. 3 TMG).

Data protection law covers all activities in relation to personal data (cf. Section 3 para. 2 to 6 BDSG). Therefore, there is no "escape" from data protection law due to the type of activity.

3 In detail and fundamentally: Eckhardt, in: Big Data in Marketing, Editor Dr. Schwarz, Haufe; Eckhardt, CR 2011, 339; Brink/Eckhardt, Editorial, ZD 1/2015 and ZD 2015, 205 et seq.

4 BGH, ruling dated 28.10.2014, IV ZR 135/15, CR 2015, 110 et seq. with Observation by Eckhardt (CR 2015, 114 et seq.)

5 The Advocate General of the ECJ gave an opinion on 05.12.2015 in this case C-582/14.

In addition to the application of data protection law, which elements of data protection law are applied is also crucial: The German Federal Data Protection Act (BDSG), or the data protection provisions of the Telemedia Act (Sections 11 et seq. TMG). **The distinction between the BDSG and the TMG is not clearly regulated by law,** so that it is in the nature of things that there are different views in the legal world. **In simple terms, the demarcation can be summed up as follows:** The data protection provisions of the TMG are applicable to Internet-specific facts and circumstances, while the rest (with the exception of telecommunications) is governed by the BDSG.[6] In the present context, the application of Sections 11 et seq. TMG is assumed.

5.2 Usage profile in online and email marketing

The data protection provisions of the Telemedia Act have a special regulation for the creation of online usage profiles for the marketing in Section 15 para. 3 TMG: *"For the purposes of advertising, market research or demand-oriented design of telemedia usage profiles, the service provider may use pseudonyms, if the user does not object to this. The service provider must point out the right of objection to the users as part of their process for providing information pursuant to Section 13 para. 1. These usage profiles may not be merged with data about the bearer of the pseudonym."*

This results in three possibilities for profiling:

- **Personal profiles:** Only permissible with consent
- **Pseudonymized usage profiles:** Permissibility under the conditions of the above-mentioned Section 15 para. 3 TMG
- **Anonymized usage profiles:** No data protection restriction since there is no application of data protection law (see above Point 5.1))

Obtaining consent theoretically presents the broadest latitude for profiling. Consent is accordingly subject to the above requirements (see Chapter 2).

In practice, the following aspects are a particular challenge in obtaining consent for the creation of online profiles:

(1) The person in question must be asked before data collection is initiated and in such a way that the consent is clear. The "one has to reckon with that" approach is not sufficient.

(2) The person in question must be clearly informed as to what specifically is to be done - i.e. how the data is evaluated and analyzed.

In the case of personalized email marketing, the use of anonymous data is often not possible.

This is because email marketing is precisely advertising in relation to specific recipients identified by their email address. In any case, data that was anonymous to date becomes personal data when assigned to an identified recipient.

6 In-depth: Eckhardt, in: Big Data in Marketing, Editor Dr. Schwarz, Haufe.

The creation of so-called pseudonymized user profiles is permitted in accordance to Section 15 para. 3 TMG under these three conditions. These three conditions must exist together.

› **Pseudonyms must be used.**
The term pseudonymization has already been discussed in Point 5.1 above.

› **The person in question must have been informed during the data collection on the right of objection against the creation of user profiles; a subsequent notification is not sufficient.**
The notification of the right of objection must also inform the person in question that user profiles will be created. The notification must be made when the person in question starts to use the service. A notification made after the start or the end of the profiling is not sufficient.

The position of the German data protection supervisory authorities with regard to Google Analytics,[7] however, indicates that a notification in the so-called privacy policy (Section 13 para. 1 TMG) on the Internet is sufficient.

› **The usage profile must not be merged with the bearer of the pseudonym.**
This means that the regulation of Section 15 para. 3 TMG is only applicable, even when the profile later does not refer to the specific person in question.

5.3 Consequences for email marketing

These provisions, in particular Section 15 para. 3 TMG, apply to all online profiles for marketing. This includes both the collection and evaluation of the opening and clicking behavior of an email recipient, as well as other forms of data collection.

The legislation provides for a possible use of personal data. The maintenance of the pseudonymization coding in the use of profiles is often a challenge. There is no standard legal solution, but the specific design must be examined in each individual case.

7 Decision by the supreme supervisory authorities for the protection of data in the non-public sector on 26/27 November, 2009 in Stralsund, structuring of analysis methods for the range measurement of internet offerings that comply with data protection provisions

6. Contract data processing with the integration of service providers

If any (external) service providers are used in the email marketing, their compliance with data protection regulations must be examined. External service providers can be software providers (in particular cloud services) for CRM and dispatch solutions, agencies, content suppliers, analysis service providers, etc. When using service providers, compliance with data protection regulations must be observed. The data protection legislation is not relevant in all cases of integration of service providers.

Whether the service provider has access to personal data is crucial for the application of data protection legislation. Which data is considered personal was already described above under Point 5.1. If the service provider has anything to do with the personal data (e.g. preparation, enriching, comparing), the application of the data protection legislation is clear. If, on the other hand, there is only a possibility of access, the question arises as to whether data protection law is applicable. The demarcation is difficult and is evaluated differently in specialist circles. Therefore, the question as to whether there should be such access - to be on the safe side - focuses on whether the service provider can actually access it, and not on whether it should or is allowed to.

In the view of the German data protection supervisory authorities, the application of data protection law is not ruled out even if only encrypted data is kept in a cloud service and the cloud provider only has access to such encrypted data.[8] This consideration is legally disputed.

6.1 Advantages of structuring as contract data processing

The typical structure for the integration of service providers with access to personal data is that of contract data processing in accordance with the provisions of Section 11 BDSG. The advantage of contract data processing is that for the data transmission to a contracted data processor, neither the legal prerequisites for data transmission (e.g. Section 28 BDSG) nor the consent of the individuals concerned must be given. This effect is considered as a so-called privileged treatment of the contract data processing and has its legal basis in Section 3 para. 8 sent. 2 BDSG.[9]

However, a prerequisite for this privilege is:

(1) The strict implementation of the provisions of Section 11 BDSG (see b) below).

(2) The data remains in the European Union (EU) or the European Economic Area (EEA) (see below 6.3).

8 Orientation aid - Cloud Computing of the Working Group for Technology and Media of the Conference of Data Protection Commissioners of the Federal Government and the Federal States, as well as the Working Group for International Data Traffic of the Dusseldorfer Kreis, version 2.0, version 10.09.2014, page 12 et seq.

9 In-depth: Eckhardt, DUD 2013, 585 et. seq.; Eckhardt/Kramer, DuD 2014, 147 et seq.

6.2 Contract data processing

Contract data processing is characterized by 3 elements:

- Instruction-based activities of service providers in relation to personal data
- Written agreement with content in accordance with Section 11 para. 2 sent. 2 BDSG

The formation of convictions by the customer in relation to the technical and organizational data protection measures taken by the contractor prior to the commencement of data processing and also subsequently on a regular basis.

The relationship that is subject to directives is given if the contractor has no leeway to make decisions with regard to the handling of personal data. To put it bluntly: In each situation, the service provider must know what to do by means of instructions from the customer. This is usually established by the description of service given in the agreement or order.

According to the "German interpretation", the Order Data Protection Agreement requires the written form within the meaning of Section 126 BGB, so that an electronic conclusion is excluded, unless the contract is concluded under use of qualified electronic signatures in accordance with the provisions of Section 126a BGB. The minimum content of the agreement in accordance with Section 11 para. 2 sent. 2 BDSG must include:

1. *"Object and duration of the Agreement,*
2. *The scope, type and purpose of the foreseen collection, processing or use of data, the data type and the circle of concerned persons,*
3. *The technical and organizational measures to be taken pursuant to Section 9.*
4. *The correction, deletion and blocking of data,*
5. *The obligations of the contractor referred to in paragraph 4, and in particular, the verification to be performed,*
6. *The possible authorization as justification for subcontract relationships,*
7. *The control rights of the client and the corresponding toleration and cooperation obligations of the contractor,*
8. *Violations against regulations for the protection of personal data or against the determinations established in the work order, to be reported by the contractor or its employees,*
9. *The scope of the authority to give instructions that the client holds in relation to the contractor,*
10. *The return of any data media provided and the deletion of the data stored at the contractor's site on termination of the contract".*

The formation of convictions in relation to the technical and organizational data protection measures taken by the contractor must not necessarily be performed by the client at the contractor's premises. The extent to which the contractor may rely on statements of the contractor is debated in specialist circles. Appropriate certifications, approval seals and audits by independent and competent third parties, which cover the entire spectrum of the order, are the preferred solution.[10]

10 In-depth: Guidelines - Data protection and cloud computing, Guideline No. 11, Competence Centre Trusted Cloud, page 19 et seq.

6.3 Cross-border contract data processing

If the personal data is transmitted across international borders or accessed from other countries (see introduction to Point 6), the admissibility of this cross-border traffic requires an additional (!) admissibility check with the data protection legislation (Section 4b, 4c BDSG).

The evaluation results in a simple dichotomy: If the data or data access remains **within the EU or the EEA,** then there is no additional requirements for admissibility checks.

If the data is transmitted or accessed from **outside the EU or the EEA,** in accordance with the provisions of Sections 4b, 4c BDSG it must be verified whether there is an adequate level of data protection for the recipient in his/her country.[11] In this case, the problem is exacerbated by the fact that the so-called privileged treatment effect of contract data processing according to Section 3 para. 8 sent. 2 BDSG (see above) is eliminated. It must also be checked if there is a legal admissibility regulation for the transmission or access.[12] As a result, a two-stage test is then required: 1. Permissibility of the transmission or access according to Sections 28 and 29 BDSG. 2. Permissibility of the transmission in the corresponding country according to Sections 4b and 4c BDSG.

11 More in detail: EuroCloud Guidelines Law, Data Protection & Compliance, http://www.eurocloud.de/2010/news/datensicherheit/eurocloud-leitfaden-recht-datenschutz-compliance.html; Guidelines – Data protection and Cloud Computing, Guideline No 11, Competence Centre Trusted Cloud, page 27 et seq.

12 The consent of all persons in question is typically excluded as a structural possibility.

6.4 Responsibility of the client

The client of the service provider must illustrate its responsibility under two aspects:
When transferring data to the service provider - even if this is done abroad - there is no exemption from the German data protection restrictions in relation to the handling of this data. To put it bluntly: What clients are not allowed to do on their own systems, they are not allowed to do on the systems of the service provider. The client remains fully responsible to those whose data are to be processed according to Section 11 para. 1 BDSG. Claims for compensation can be made against him/her for errors made by the service providers (Section 278 BGB).

The client also bears the responsibility for the correct structure of the Contract Data Processing Agreement. This results from Section 11 BDSG. This is illustrated by the threat of fines in Section 43 para. 1 no. 2b BDSG, which are only imposed against the client. However, fines may be imposed against the service provider in the case of invalid contract data processing in particular pursuant to Section 43 para. 2 no. 1 BDSG, or as a participant in the event of infringements by the client. If the service provider has specified this in the Contract Data Processing Agreement, this could result in a claim for compensation of the client. In brief: It is in the interest of both that contract data processing is properly structured.[13]

13 In 2015, for instance, the Bavarian Data Protection Authority (BayLDA) established five-digit fines in the event of inadequate order placement (press release by BayLDA, "Contract data processing without proper contract can be expensive", 20 August 2015).

7. EU General Data Protection Regulation - an Overview

The General Data Protection Regulation (GDPR) was published on 05 April 2016 in the Official Journal of the European Union14, entered into force on 25 May 2016 and is applicable in accordance with Article 99 from 25 May 2018 on. The legislative process initiated on 25 January 2012 is thus completed.[15] The GDPR has a comprehensive regulation of data protection.[16]

EU regulations have priority of application over conflicting national law. Divergent national regulations are only possible in so far as the GDPR itself contains flexibility clauses for this.[17] To put it bluntly: GDPR replaces the national data protection regulation and provides exceptions only in certain sectors.

The regulations of GDPR, as well as national laws, are subject to interpretation and are not always clear and coherent in every respect. Precisely because of the European legislative process there are some outstanding questions to be clarified.[18]
T
he following is an overview of the emerging consequences on email marketing:

7.1 Limited continued validity of consent after 25 May 2018?

Recital 171 GDPR essentially provides that up to 25 May 2018, all processing of personal data must be adapted to the GDPR.[19] There are no safeguards after 25 May 2018. For consent, the following is regulated:

"... if the processing is based on a consent in accordance with the provisions of Directive 95/46/EC, it is not necessary that the person in question must grant their consent, when the type of the already granted consent complies with the terms of this Regulation, so that the person responsible can continue the processing after the date of application of this Regulation. ..."

Accordingly, a consent is still effective if two conditions are met:

1. The consent meets the requirements of Directive 95/46/EC. These are requirements which the BGH has already mentioned in its decision "Consent in Telemarketing II"[20] and "reflects" it in Art. 4 no. 11 GDPR.
2. The "conditions" of GDPR have been met. In accordance with the wording, these are only the indications given in Arts. 7, 8 GDPR. The transparency requirements pursuant to Arts. 13 and 14 were then not requirements for effectiveness.

14 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119/1 of 4 May 2016.

15 About the background: Eckhardt CR 2012, 195 et seq. on the former proposal of the EU Commission

16 In detail and fundamentally: Eckhardt/Kramer, Current Data Protection – Special Report EU General Data Protection Regulation, TKMmedia

17 In detail and fundamentally: Eckhardt/Kramer, Current Data Protection – Special Report EU General Data Protection Regulation, TKMmedia

18 In detail and fundamentally: Eckhardt/Kramer, Current Data Protection – Special Report EU General Data Protection Regulation, TKMmedia

19 In detail and fundamentally: Eckhardt/Kramer, Current Data Protection – Special Report EU General Data Protection Regulation, TKMmedia

20 BGH, judgment dated 25 October 2012, I ZR 169/10, MMR 2013, 380 et seq. Note Eckhardt (Page 382 et seq.).

7.2 Regulation of consent

The regulation of consent is in multiple parts of the GDPR. The concept of consent is defined and the basic requirements are established in Art. 4 no. 11 GDPR. This is not exactly new to the previous understanding of the term, in particular on the basis of the decision "Consent in Telemarketing II"[21] of the BGH.

Art. 7 GDPR establishes more "conditions" for a consent. The stipulated principles are not entirely new, but will nevertheless have to be assessed in detail as to what extent this brings changes to the existing legal situation. What is new is the general obligation to inform the person in question, prior to granting consent of the right to revoke the consent (Art. 7 para. 3 sent. 3 GDPR). Particularly in the case of advertising consent, this is normally done due to Section 28 para. 4 sent. 2 BDSG, Section 7, para. 4 no. c UWG as well as in the case of electronic consent due to Section 13 para. 3 TMG.

Art. 8 GDPR contains "conditions for the consent of a child in relation to the services of the information society". These are to be observed in relation to children in any case. Whether any action must be taken in general for consent is still to be clarified. In practice this means that: It must be checked whether, and if so, what shortcomings there are among the existing consents to the specifications of the GDPR. On this basis, it must be evaluated whether and when the request for consent must be adjusted and if any changes are necessary for older consents.

21 BGH, judgment dated 25 October 2012, I ZR 169/10, MMR 2013, 380 et seq. Note Eckhardt (Page 382 et seq.).

7.3 Transparency requirements

Arts. 13, 14 GDPR contains general information obligations to be fulfilled proactively. The regulations are different for legitimacy issues and for consent. Art. 13 GDPR is relevant in the case of the collection of personal data from the person in question and Art. 14 GDPR if the personal data has not been obtained from the person in question.

The information requirements have been extended in comparison with the previous obligations in the data protection laws to a significant extent. In any case, this requires adaptation.

Art. 21 GDPR contains its own regulation on the right of opposition of the person in question. However, this does not apply to consent.

Even if the breach of the obligation to inform does not invalidate the consent, infringement is sanctioned with a fine of up to EUR 20 million, or 4% of the total worldwide annual turnover obtained in the preceding business year, whichever is the greater, (Art. 83 para. 5 GDPR).

7.4 Profiling

There are no special regulations for profiling comparable to those in Section 15 para. 3 TMG for marketing. Art. 22 GDPR deals with profiling, as long as it is an integral part of an automated decision, which has legal effects for the person in question or affects them in a similar way. This is typically not the case for a marketing profiling, but it

must be verified in each individual case. As the legal basis for a marketing profiling under GDPR the general interest is taken into consideration in Art. 6 para. 1 lit. f et seq. GDPR. A balancing of interests must take place here. If personal data is to be used for a change of purpose for the marketing profile, Art. 6 para. 4 GDPR must be taken into consideration in the verification process.

The transparency requirements of Arts. 13, 14 GDPR (see above), and particularly the regulations concerning the right of opposition in Art. 21 GDPR (see above) should be observed for such a profiling. Whether a breach of the transparency provisions makes the processing illegal will certainly be the subject of discussions. This was denied for previous configurations of BDSG, but this is not the only standard for the EU compliancy of GDPR.

7.5 Contract data processing

Contract data processing (as it is called in GDPR) is regulated in Art. 26 GDPR. The preferential treatment effect is also laid out in Art. 4 no. 10 GDPR, since the order processor is not considered a third party. The discussion as to whether this is sufficient for the privilege effect has already begun.

The content structure of the contract data processing is comparable to that regulated under Section 11 BDSG, although, of course, there are differences and their impact should be examined in detail.

However, one novelty is that according to Art. 82 GDPR the order processor is jointly and severally liable in addition to the client (Art. 82 para. 4 GDPR). However, there is a possibility of limiting this for the order processor. Whether any action must be taken by the service provider is still to be clarified.

Another novelty from a German point of view is the so-called "joined controllership" in Art. 26 - meaning: jointly responsible for the processing. The question here is to what extent the service provider will be jointly responsible together with the client and there is no client - contractor processor relationship. A prerequisite of Art. 26 para. 1 sent. 1 GDPR is that the purposes and processing methods should be jointly determined. In practice, the question will arise as to how close a relationship is required for this purpose. Some action must be taken by the service provider here too.

7.6 E-Privacy Directive (Directive 2002/58/EC)

Art. 95 GDPR does not impose any additional obligations on individuals or legal entities in respect to processing in connection with the provision of publicly available electronic communications services in public communications networks in the Union, in so far as they are subject to particular obligations in Directive 2002/58/EC, which have the same objective.

Simply put: The national legislator can still establish regulations within the scope of the Directive 2002/58/EC. In Germany, this Directive is primarily in the data protection provisions of the Telecommunications Law (Section 91 et seq. TKG). However, not only requirements arising from this Directive are

regulated, the scope of application is also defined differently in the TKG than in Art. 95 GDPR. Some legislative action is required from the national legislator in order to clarify this question.

More exciting for the present context, however, is the discussion on whether the specifications of the so-called Cookie Directive, which is ultimately a directive amending Directive 2002/58/EC, were already implemented in the data protection provisions of the TMG, or not. If so, the data protection provisions of the TMG could possibly continue to apply under GDPR. Otherwise, the data protection provisions of the TMG (Sections 11 et seq. TMG) are "displaced" by GDPR. Some legislative action is required from the national legislator in order to clarify this question.

7.7 Conclusion

The EU GDPR implies change and adaptation requirements, which must be performed by 25 May 2018. However, a careful analysis of the situation must be performed beforehand. In particular, this must include a clarification of the interpretation and application questions of the GDPR. To put it bluntly: Blind activism is just as bad as "sitting back and waiting".

8. What should be observed in other countries in email marketing

8.1 Legal aspects in Switzerland

Whereas the sending of advertising emails has long been strictly regulated in the EU and particularly in Germany, the Swiss legislature did not create corresponding specific statutory bases until 2007. These regulations are firstly to be found in the UWG (Gesetz gegen den unlauteren Wettbewerb [Act Against Unfair Competition]) (UWG, Art. 3 lit. o), and secondly in the FMG (Fernmeldegesetz [Telecommunications Act]), Art. 45a). The UWG fundamentally regulates the conditions for the sending of commercial emails. The FMG records which measures the telecommunications provider has to take to combat spam.

The state itself (State Secretariat for Economic Affairs, SECO, www.seco.admin.ch) can also take measures against spammers at home and abroad if enough people complain.

After the revision of the DSG (Schweizerisches Datenschutzgesetz [Swiss Data Protection Act]) of 2006 - the relevant rules entered into force in 2008 - the data protection regulations gained relevance in the case of email marketing. On the one hand, Art. 3 lit. o UWG does not apply in advertising emails, because it is not automated mass advertising, but on the other hand it supplements Art. 3 lit. o UWG in the case of mass advertising. In connection with email marketing, Art. 4 para. 3 and para. 4 DSG is particularly

relevant. Art. 4 para. 3 DSG stipulates the so-called precept of purpose linking.

Personal data may only be processed for the purposes indicated on obtaining the data or for the purposes discernible under the circumstances. Art. 4 para. 4 DSG establishes the so-called requirement of transparency. The procurement and processing of personal data and the purpose of the processing must be recognizable for the person in question. If these two data processing principles are not respected, there is a breach of personality rights. In this case, according to Art. 13 DSG, a justification is necessary (e.g. the consent of the person in question or an overriding interest of the data processor). In the event of a breach of the data processing principles, as a rule, consent is necessary for email marketing.

This overview of the legal provisions relevant for email marketing shows that the legal requirements in Switzerland are far less detailed than, for example, in Germany.

There is much more scope for interpretation. What is actually permitted, and what is not?

Mailing of advertising emails to non-customers

The "mass mailing of advertising via the Internet or telecommunication services" to non-customers is legally permissible if the following requirements are met:

- Prior to the receipt of the email, the recipient must have expressly consented (opt-in principle) (see also "registration methods").
- The sender must be clearly recognizable. The address must be correctly given; the identity must not be hidden or falsified.
- Each advertising email should contain a clearly discernible, free-of-charge, and simple unsubscribe option (e.g. unsubscribe link with confirmation of unsubscribe, possibly a link to the online unsubscribe form).

Consent is also necessary from the point of view of data protection laws. In the case of advertising emails to non-customers, the data protection legal transparency principle is regularly not respected.

Mailing of advertising emails to existing customers.

For email advertising to existing customers, Art. 3 lit. o UWG makes provision for a certain alleviation. A recipient is considered as an "existing customer" when there is an economic relationship between them and the advertising company, i.e. a purchase must actually have taken place (service or product). When mailing advertising emails to such existing customers, **no opt-in is required** if the following conditions are met:

- There is a link between the service purchased at a particular time and the service advertised (advertising of comparable products or services).
- No third-party services are advertised.
- When mailing of advertising emails to existing customers, the sender must be clearly discernible, and each email must contain an easy-to-find, free-of-charge unsubscribe option (see above).

If the above-mentioned prerequisites are not fulfilled - when, for example, information on third-party products is to be sent to the existing customer - the same requirements as for the mailing advertising emails to non-customers must be fulfilled.

Methods of registration

In Art. 3 lit. o UWG, the Swiss legislator has refrained from regulating the form and provability of the registration. The sender is, therefore, basically free to choose one of the registration methods described above. The only mandatory requirement is that the recipient "expressly" gives its consent. When collecting offline registrations (e.g. at trade fairs, by telephone, or via physical registration forms in the sales store), there is no provision that regulates the provability and storage obligation in detail. Ultimately, the sender must ensure that the recipient expressly consented to receipt in the advertising email.

In order to comply with the opt-in principle, there are the following online registration methods in email marketing:

› Single opt-in:
Subscribers register online expressly by clicking on the corresponding check box and entering their email address (and possibly other data). The registration is merely confirmed on a following page of the registration page. This method of registration is generally not recommended.

› Confirmed opt-in:
Subscribers register online expressly by clicking on the corresponding check box and entering their email address (and possibly other data). The registration is first confirmed on the following page and then re-confirmed by email.

A confirmed opt-in (single opt-in with email confirmation without a confirmation link) is allowed from a fair legal point of view, but in terms of data protection law, it has some inherent risks. As explained in more detail below (see double opt-in), the company processing the personal data must verify the accuracy and ensure that the recipient has given his/her consent to the receipt of email advertising. There is a certain risk of abuse with the confirmed opt-in procedure. It cannot be ruled out, for instance, that someone provides a third-party email address and thus orders a newsletter to a third-party email address. It is impossible for the company with the confirmed opt-in to ascertain whether the registration was actually made by the owner of the email address.

› Double opt-In:
The so-called "double opt-in procedure" has gained ground in practice, in particular in relation to the Data Protection Act. The double opt-in is a process in which a customer "doubly" issues his/her consent (in two steps). In a first step, the recipient provides an email address in order to receive e.g. a newsletter (step 1). The advertising company will then send a confirmation email with a confirmation link to the email address provided by the recipient and the recipient confirms (by clicking) on the confirmation link his/her desire to receive the newsletter (second step).

Although from the point of view of fair trade laws, consent is already granted in

the first step; it is recommended to use the double opt-in approach in relation to data protection law. Ultimately, the sender must ensure that the recipient expressly consented to receive the advertising. This can only be ensured with the double opt-in process.

"Tell-a-Friend" functions

In Switzerland, the so-called "Tell-a-Friend" functions are common and widely recognized as permissible. At least messages that are sent by this function are not classified as mass advertising within the meaning of Art. 3 lit. o UWG. In accordance with the legislative material, mass advertising is messages that are sent in an automated manner. Advertising messages that require a human effort - in the case of "Tell-a-Friend" the input of individual email addresses - are not regarded as mass advertising.

Purchased Addresses

A frequent question is: "Is it permitted to send emails to purchased / rented addresses?"

Many advertising companies are operating in a gray area under Swiss law. Many advertising companies assume that they may send advertising emails to purchased addresses without further ado. However, this is not correct.

The particular difficulty in sending advertising emails to purchased addresses is that the advertising companies did not obtain the data directly from the person in question. Without the appropriate information, it is not discernible for the person in question that the purchased email address was sold to third parties for marketing purposes. No information would mean a violation of Art. 4 para. 4 DSG, which can only be justified regularly through consent (Art. 13 DSG). Consent is already absolutely necessary under Art. 3 lit. o UWG. Ideally, an informed consent should be obtained by the data provider at the time the data is collected.

The extent of the information in connection with the consent, as already mentioned, is not sufficiently clear from either Art. 3 lit. o UWG or from the Data Protection Act. The client or persons in question must be able to form an idea regarding the circle of the data recipients. If the provider of personal data wants to forward the addresses to a unrestricted circle of recipients, the requirements of the consent are correspondingly higher. Information and consent must be explicit here. If the information and consent is contained in general terms and conditions, the circle of third parties should not be unexpectedly large or unexpectedly composed. A transfer of addresses by means of consent and the information in the general terms and conditions may therefore be permitted e.g. when forwarding to other group companies, but not to an unlimited number of third parties.

In view of Art. 3 lit. o UWG, it is also important that the advertiser does not rely on the assurance of third parties that there is adequate consent.

Procurement from publicly available sources

Many advertising companies assume that they may use advertising emails obtained

from public sources without any usage restrictions. However, this frequently made assumption is not correct.

Email addresses can be collected, in particular by Internet research. In this case, the sender of advertising emails can neither invoke a (implicit or explicit) consent, nor a pre-existing business relationship. Therefore, there are no grounds for permissible advertising sent by email (pursuant to Art. 3 para. 1 lit. o UWG).

From the point of view of data protection, the use of email addresses obtained from public sources for advertising emails is also problematic. Obtaining addresses from public sources is not recognizable for the person in question so that Art. 4 para. 4 DSG is always violated. At first glance, it seems possible under data protection law to invoke that the persons in question have made their email addresses publicly available and therefore sending them advertising emails (according to Art. 12 para. 3 DSG) is presumably not a breach of privacy. This presumption applies only to data processing within the framework of the purpose of the disclosure apparent from the circumstances of the person in question. A person who reveals their email address on a website is not necessarily inviting the sending of mass advertising.

The context of the publication of the address can also result in that the purpose of the publication covers the sending of targeted advertising e.g. registration of the email address in yellow pages, commercial directories, etc.

Caution: Market place principle

As already mentioned, Swiss legislation is less detailed than that of Germany. It is therefore understandable that most Swiss companies do not heed the more detailed foreign specifications.

However, there is a not entirely harmless "drawback" that Swiss companies should be aware of: If a Swiss company sends emails to recipients abroad, it is fundamentally subject to compliance with foreign legislation (and thus mostly more detailed) pursuant to the principle of "market place principle".

What does the term "market place principle" mean? A market place is a place where influence is to be exerted on the recipient from a marketing perspective. Indications to define a market place are:

- Country code of the email address (e.g. @examplemail.de),
- Language of the email,
- Country reference of the advertised product (e.g. German Internet sites)

If the definition above is strictly applied, it must be assumed with subscribers for a German-language newsletter that they can also come from Germany. As a mandatory field during registration, only the email address can be collected. Moreover, the company is obligated to be able to prove the registration – irrespective of whether it was completed offline or online – in a credible and seamless manner.

Of course, factors such as the size of the advertising company and the question of

whether the company operates at a regional, national, or even international level, play a major role in the question regarding the importance of this regulation. With a purely locally active small company, it is probably only to be assumed in the rarest of cases that customers from Germany subscribe to the newsletter, then "forget" it, and subsequently complain about the unsolicited sending of emails.

However, every company that wants to use the benefits of email as a medium to acquire and retain customers should consider in detail whether it wants to "only" be right at the limit of the statutory specifications with regard to its communication policy, or whether the fundamentally positive agreement with (potential) customers should set the signal for the communication instead.

Penalties for the violation of the legal specifications

Those who willfully commit unfair competition pursuant to Article 3 UWG will on request be punished with imprisonment for up to three years or with a fine (Art. 23 UWG). However, as yet there is no legally enforceable Federal Supreme Court judgment in Switzerland on this offense (Art. 3 lit. o UWG). As far as can be seen, only the Cantonal Court of Lucerne dealt with this issue in a decision of 01 July 2014 (LGVE I no. 6 2014). A recipient of an advertising email had filed a criminal complaint against the advertising company. The public prosecutor had dismissed the criminal proceedings. The Cantonal Court had confirmed this decision on appeal. In connection to the judgment, the Cantonal Court had ruled that no double opt-in was required by law. The case to be evaluated, however, shows why this registration method is recommendable. In the said case, the recipient of the advertising email claimed that he had not provided his email address, nor given his consent. The advertising company however affirmed that the email address had been entered on their website in relation to receiving the newsletter.

With a few exceptions, there are no effective sanctions for violations of the Data Protection Act in the applicable law. There are no criminal sanctions in the current Data Protection Act for violations of the transparency requirement, if it is just "normal" data (Art. 34 DSG). It is a different case if, when obtaining personal data from third-party sources in addition to email addresses which qualify as "normal" personal data, particularly sensitive data is collected and a personality profile is created. In this case, Art. 14 DSG provides for an active information requirement. Violations of this obligation can be sanctioned with a fine (Art. 34 para. 1 DSG). In addition, the person in question may at any time initiate civil proceedings (Art. 15 para. 1 DSG). They may request that further processing of the data be prohibited or that the data collected be deleted.

In future, the sanctions in the event of data protection violations must be extended. In particular, the Swiss Federal Data Protection Commissioner should be given the competence to impose substantial fines for violations of data protection in the event of infringement of its recommendations. At present, the revision project is only at the stage of expert advice. No concrete

preliminary draft has yet been prepared. If the revision is passed in the future and the revised Swiss Data Protection Act, as is to be expected, is also based on the European General Data Protection Regulation, advertising companies must observe the Data Protection Act with much more attention than is currently the case.

The only important factor is the law

Even if enforcement of the Swiss Spam Act is more theoretical than practical, advertising companies should observe the following: (potential) customers who feel "spammed" demonstrably and very quickly develop a defensive attitude towards the advertising company.

Therefore, it is indeed recommended for Swiss companies that they comply with the substantially more detailed legal requirements in Germany and the double opt-in process; this firstly ensures that all subscribers, whether they come from Switzerland or neighboring countries, are written to in a legally compliant manner. Although the recipient base may possibly remain slightly smaller due to the use of the double opt-in registration method, this only includes readers who are really interested in the sender's offer and will also react accordingly to its emails.

The following checklist shows which conditions a company must fulfill in the mailing of marketing emails in Switzerland and which conditions should be additionally and voluntarily fulfilled. The checklist is not to be viewed as exhaustive. Medium-sized and larger companies are advised to consult a specialist in communication law for the formulation of the email marketing guidelines.

Checklist

- ✔ Correct and unmistakable sender address (true identity)
  - › Mandatory
- ✔ Previous express consent or existing commercial relationship to the recipient (recipient is customer)
  - › Mandatory
- ✔ Easy and highly visible rejection option for future mailings (the same means of communication, no further costs); e.g. unsubscribe link, unsubscribing by email reply
  - › Mandatory
- ✔ Online consent: Any check box that reflects the consent to receive the advertising emails of the sender must be expressly clicked (no pre-selected check boxes)
  - › Mandatory
- ✔ Unsubscribed recipients are no longer contacted by email
  - › Mandatory
- ✔ Emails to existing customers: No sending of third-party advertising without their express consent being obtained beforehand
  - › Mandatory
- ✔ No automated advertising emails to email addresses which have been obtained from public sources
  - › Mandatory
- ✔ When sending advertising emails to purchased addresses, it is essential to obtain a written commitment by the seller that the persons in question have given valid consent. Ideally, the advertising companies should verify the validity of consent at random intervals
  - › Recommended

- ✔ Emails to existing customers: No advertising of own products/services without the corresponding express consent being obtained beforehand.
  › Recommended
- ✔ Complete legal notice with offline contact option (address, telephone number) and a guarantee of the sender being available
  › Recommended
- ✔ Online registration solely via double opt-in (traceability!)
  › Recommended
- ✔ Consent obtained offline is saved/filed (traceability!)
  › Recommended
- ✔ Dispensing with sending emails to customers whom you have had no contact with for a lengthy period of time.
  › Recommended

Other useful information on the topic:

› Website of the Federal Data Protection and Information Commissioner (FDPIC):
http://www.edoeb.admin.ch/datenschutz/00683/00803/00816/index.html?lang=de

› **http://www.edoeb.admin.ch/dokumentation/00612/00660/00687/index.html**

› **www.kommunikationsrecht.ch**

8.2 The legal situation in Austria

In Austrian law, the legal framework for email marketing is shaped by various statutory regulations which are based in part, like the German regulations, on the implementation of the corresponding EU directive. The practical implementation of these regulations deviates considerably in part from German law. The following overview is limited to the Austrian regulations on the unsolicited sending of electronic mail as well as obligations to inform and data protection provisions associated there with. Special regulations in sector and industry-specific laws are not examined in this overview. There are parallels between Austrian and German data protection law, whereby Austrian law does not foresee any special equivalent to the data protection provisions in the German Telemedia Act (TMG).

Introduction

The obstacles for the permissible sending of electronic mail are set out in Section 107 paras. 2, 3, and 5 **TKG (Telekommunikationsgesetz [Telecommunications Act]) of 2003.** Emails to consumers (B2C) and companies (B2B) are affected by these provisions. Accompanying provisions are contained in the ECG (E-Commerce-Gesetz [E-Commerce Act]).

Permissibility of email marketing – principle of opt-in

Like German law, Austrian law makes provision for an "opt-in procedure" in principle. According to Section 107 para. 2 TKG 2003, **consent** is required from the addressee of the email to the mailing if

- the mailing is done for direct advertising purposes or
- is addressed to more than 50 recipients.

The Austrian courts define direct advertising in a similarly generous manner to the German courts so that newsletters, in particular, are covered. The recipient should be protected from a breach of privacy by unwanted electronic communication as well as from an expense or other charges. According to the VwGH (Österreichischen Verwaltungsgerichtshof [Austrian Administrative Court]) [VwGH, 19 Dec. 2013, 2011/03/0198], the provisions of the TKG 2003 are also applicable to canvassing for elections, since a corresponding scornful effect is to be obtained. Providing an email address in a public online directory of members is not sufficient here as consent.

If email is sent to more than 50 recipients, private emails are also subject to the text of the TKG 2003. Even if the importance of the practice is low - from a purely legal point of view - the requirements of the law (e.g. unsubscribe option) must also be met.

The consent required in accordance with the legislation must be obtained before the emails are sent out. There are **no formal requirements** for the agreement, which means that even a conclusive consent would be valid in principle. The **burden of proof** for the existence of consent from the recipient lies with the sender of the email. This results in the obtaining of the consent having to be organized in such a manner that it is provable. In Austrian and German law there are comparable problems of proof (see Chapter 2.10 above on the burden of proof in German law). The double opt-in lends itself here in which, for instance after the subscription to a newsletter, an advertising-free email is sent with the question as to whether the recipient really does want to subscribe to the newsletter. The resulting confirmation is relevant. However, there are no legal requirements relating to the nature of the registration procedure. If the registration procedure is too complicated, there is always the associated risk that, ultimately, less registrations are generated.

In order to determine the applicable law in each case, the **recipient country principle** is applied in the EU zone. So the legislation to which the recipient of the email is subject must always be applied. This "crime scene fiction" is regulated in Austria in Section 107 para. 6 TKG 2003. The VwGH [VwGH, 19 December 2013, 2012/03/0052] has stated that in accordance with the **protection principle** of the regulation, it does not depend on the location of the server. Even if it is not clear where the email was ultimately retrieved, this (according to the Constitutional Court) is no excuse for the violation of the relevant legal provisions.

Permissibility of email marketing – "opt-out" as an exception

Section 107 para. 3 TKG 2003 – comparable to the German Section 7 para. 3 UWG – makes provision for an exception to the opt-in principle with existing customer relationships. The background to this is that both the Austrian and the German regulation are based on a European directive.
An **exception to the need for consent** exists pursuant to Section 107 para. 3 TKG 2003, if

- the sender has received the contact information for the message in connection with a sale or a service to its customers, AND
- the message is sent to directly advertise the company's own similar products or services, AND
- the recipient clearly and distinctly has, during collection and also during each transmission, the possibility to reject such use of this electronic information easily and free of charge,AND
- the recipient has not rejected the mailing from the outset, in particular, not as the result of entry in the list named in Section 7 para. 2 of the ECG (E-Commerce-Gesetz [E-Commerce Act]).

Said requirements must all be met at the same time ("AND"). If one of the requirements is not met, the exception does not apply and consent is necessary. If the exemption clause is applied, however, Section 7 para. 1 ECG is applicable, in accordance to which commercial communications should be clearly recognizable as such in each case upon receipt by the recipient.

Rejection from the outset – the last named requirement – must not necessarily have been declared to the sender. The objection can also be made by entry in the list named in Section 7 para. 2 ECG, the so-called "ECG List" - (Robinson List). Consequently, at least a comparison with this "blocked" list is necessary before each mailing. This list is kept by Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH). The list can be requested in electronic form from RTR-GmbH and then compared. There are three variants for the comparison of this "ECG List" (as of Sept. 2016 at https://www.rtr.at/de/tk/TKKS_ECGListe). With all methods, it should be ensured that the registered parties are not named to the potential sender with their plain-text names. The special feature of the Austrian variant of this "blocked list" lies in the fact that it is anchored in the law and thus enforceable to a far greater extent. Although this does not liberate the registered persons permanently from spam, it is nevertheless effective. In many other countries, Robinson Lists are kept by clubs or similar associations, which are either only valid for its own members, or require a voluntary submission of the advertiser. That is not the case in Austria. Since, apart from existing customer relationships, which, in general, use the principle of prior approval, the "ECG List" is withdrawn from the scope of application in all other cases.

Requirements with regard to content

With direct advertising, according to Section 107 para. 5 TKG 2003, the **identity** of the sender or the client of the emailing may not be concealed or dissimulated. As in Germany, the recipient must also have the possibility at any time, to be able to unsubscribe, for example, from a newsletter easily and free of charge. The possibility must be clear and precise, but there are no specific procedural requirements. If there are several steps to this and a user account password has to be entered, this could be classified in the future by a court as "too difficult". There are no legal obligations arising for the recipient that he/she must adhere to the instructions of the sender. If an email is simply replied to, this is sufficient as an unsubscribe request. In

addition, according to Section 107 para. 5 TKG 2003, each individual email must always include an authentic address to which the recipient can **address** a request for the suspension of such messages. This is comparable to the German Section 7 para. 2 no. 4 UWG.

Information Requirements

According to the Austrian Section 24 MedienG (Mediengesetz [Media Act]) and Section 5 ECG, a **legal notice** must be included in the email. The Media Act is applicable to email advertising (periodic or recurring electronic medium) pursuant to Section 1 para. 5a lit. c, provided that emails are sent at least four times in the calendar year in a comparable design. The scope of application of the ECG is very broad so that online product advertising is sufficient to be included. For the fulfillment of the legal notice obligation, it is sufficient just to integrate the link to the legal notice in the email, since there is no requirement that the message itself contains all of this information. Section 25 of the Media Act also requires a disclosure, which can be covered with a legal notice. This disclosure requirement is primarily of importance for legal entities, since in the case of natural persons, the legal notice corresponds to Section 24 MedienG. The mandatory information therefore differs depending on the legal form of the company. In accordance with Section 25 para. 5 MedienG, there is an exception for emails (newsletters) which contain no information extending beyond the presentation of personal life, especially not obviously and primarily aimed to influence the formation of public opinion. In this case, the obligation of disclosure is considerably restricted and very little mandatory information must be given. Section 26 MedienG standardizes the obligation that paid announcements in the email must be explicitly recognizable as such in order to avoid any doubts about their character.

Moreover, the provisions of Section 14 UGB (Unternehmensgesetzbuch [Austrian Commercial Code] for "business documents and order forms" is also applicable to emails. The provision must be applied to all companies registered in the Commercial Register and again has different regulations depending on the legal form of the company. The minimum information coincides to a large extent with the MedienG, but must be included directly in the message. Basically, this is legal information pertaining to the company's commercial registration and structure. Section 14 para. 4 UGB contains a special regulation for existing business relationships.

Data Protection

If personal data is (also) to be analyzed, the DSG (Datenschutzgesetz [Data Protection Act]) 2000 must be observed. In order to intervene in the **fundamental right to data protection**, certain principles of data processing must be fulfilled. In particular, the data must be fairly and lawfully processed; processed for limited and explicit purposes necessary for the achievement of the purpose, and not stored longer than necessary. An intervention may only take place to the extent necessary and using the least invasive methods to achieve the purpose.

If these requirements are met, Section 8 para. 1 DSG is applicable. If there is no statutory authorization or obligation, no vital interests of the person in question safeguarded, if the data is not generally available or is to be used mainly in the interest of the client, the person in question must give their consent in any case. Section 9 DSG contains far more stringent requirements in the case of sensitive data.
These data protection legal obligations should be observed from the first contact with personal data. In most cases, it is more practical to obtain consent for using the data, but an explicit data privacy notice is recommended. This can also be resolved with a check box on web sites.

Tell-a-Friend function

In Austria, Tell-a-Friend advertising should be done with caution; the BGH ruling of 2013 can serve as an orientation aid. The OHG (Oberster Gerichtshof [Austrian Supreme Court]) has already spoken on this subject in 2009 [OHG 9.6.2009, 4 26/09s] and classified a "Bonus Program" initiated by an insurance agent, who offered his customers a refund of their (own) insurance premium for the recruitment of two other insurance customers, as a "snowball system". "Snowball systems" are prohibited in Austria in accordance with Section 27 UWG. Using your own customers as recruiters can therefore in individual cases be considered at least as **unfair.**

Possible sanctions

A special characteristic in Austria is that in Section 109 para. 3 no. 20 TKG 2003, a **determination of the administrative offense** is provided for, according to which those who send emails in contravention of Section 107 para. 2 or 5 TKG 2003 can be punished with a fine of up to EUR 37,000. In addition to willful intent, negligence is also sufficient to initiate the sanction. **Negligence is automatically assumed when the prohibition standard is insinuated.** In practice, this results in the sender itself having to become active to discharge itself. For this purpose, facts must be submitted and evidence furnished. General assertions are not sufficient to nullify the assumption of negligence. The occurrence of a risk or damage is not a requirement. Repeated offense can increase the fine pursuant to Section 109 para. 5 TKG 2003.

As in Germany, there is also the threat of claims for injunctive relief or compensation. The reaction to such claims, in particular to warnings, is similar to that in Germany. Nevertheless, checking and appraisal should be done in all cases by a specialist, as there are deviations from German law. In particular, there is the risk that the costs to be reimbursed to the counterparty are higher than in Germany.

Both private individuals and commercial companies who are the recipients of the email can file a claim for injunctive relief arising from Section 354 ABGB (Österreichisches Allgemeines Bürgerliches Gesetzbuch [Austrian Civil Code]) which is based on the breach of general personality rights due to intervention in the private sphere.

In particular, competing companies - competitors of the sender - can file a claim against the sender pursuant to Section 14 para. 1 in conjunction with Section 1 UWG

of Austria for injunctive relief and pursuant to Section 16 para. 1 of the UWG for damage compensation in the event of culpability.

9. Our recommendation: Certified Senders Alliance

The central white list "Certified Senders Alliance" (CSA), launched by eco - Association of the Internet Industry and the German Dialog Marketing Federation (DDV) in 2003, offers commercial mass senders and companies an effective solution for avoiding delivery problems in their email campaigns. The positive list ensures that recipients also receive emails that they have requested or require for a transaction. Primarily mass mailings such as newsletters, but also transaction emails (e.g. invoices, login confirmations, order confirmations, etc.) frequently land in the spam folder, possibly filtered out by the spam filters by mistake, (so-called false positives) and thus frequently remain hidden to the recipient. For the companies concerned, this can result in loss of earnings, and in an annoying experience for the user.

With the CSA white list, ISPs can optimize the delivery of incoming emails to their customers in order to continue to protect them effectively against spam. With a CSA certification, senders ensure that they identify themselves as trustworthy and reputable towards the ISPs affiliated with the CSA and thus avoid delivery problems as the result of a poor reputation.

CSA-certified senders are subject to strict approval criteria. Certified service providers also forward the CSA criteria via their general terms and conditions of business to their customers. The approval criteria require the fulfillment of high technical standards and legal specifications that the CSA develops together with the participants in a continuous process.

- The CSA legal criteria are in line with the EU legislation currently in force. Any commercial emails sent within the EU Member States must meet these criteria.

- The technical criteria have been developed on the basis of feedback from the ISPs, technology partners, and senders and are updated when neccesary in order to conform to current requirements. Examples are the DKIM signing of all messages as well as the use of List Unsubscribe Header, to name just two of the technical criteria.

In addition, there are a number of mechanisms that prosecute senders who violate the existing rules. The certification and complaints committee monitors the inclusion of new senders and compliance with the rules. The operational experience to date shows that the strict requirements are paying off. The number of incoming complaints is – when viewed relative to the dispatch volume of the certified senders – gratifyingly low. In individual cases, however, the certification and complaints committee must impose or confirm sanctions in order to preserve the quality of the white list. In turn, these sanctions help the sender concerned to identify and eliminate weak points in its own processes or those of its customers and thus avert greater damage in a timely manner.

In order to preserve the high quality of the white list, not only the legally impeccable audit and its control over the complaints management are necessary. In addition, the technical criteria also have to be reviewed on a regular basis. Thus, the most important criteria of the sending mail servers are reviewed automatically on a daily basis and recorded in a report. This report also contains additional tests on whether there was anything negative noticeable in the sending characteristics of the mail servers, both to provide information to the certified senders but also to gain indications of problems during sending. This is, therefore, also an additional added value that participation in the CSA offers.

The CSA is established today not only on the national market but also on the international market, and since the start of its operational service, has enjoyed a constant increase in acceptance, which in turn has a positive effect on the growth of the CSA. Expressed in figures, the CSA now includes more than 100 certified ESPs and other companies from 11 different countries. The ISPs affiliated with the CSA cover more than 500 million email accounts. In addition, renowned technology and cooperation partners participate in the CSA who increase the reach of the CSA further and provide the CSA with important instruments for the monitoring of the senders. For years, the CSA has been the most well-known and most widespread reputation standard in Germany, and now also worldwide, and thus a great success for the international Internet economy.

The CSA also offers additional services such as workshops in which experts marketers provide input on the legal framework in the optimization of email communication in the marketing management sector to ensure legally compliant and effective email campaigns.

An updated list of the participants and partners as well as all other information regarding the CSA can be found at **www.certified-senders.eu.**

10. Opt-in or opt-out – What applies in the individual countries?

With the international mailing of advertising emails, the following decisive question arises for the sender: In the country where the recipients are located (target country), does the opt-in principle (prior consent required) or an opt-out regulation apply (unsubscribe option sufficient). The decisive factor in the assessment of the lawfulness of the mailing activity is the legal position in the respective target country. Opt-in applies in all Member States of the European Union and in Norway, Liechtenstein, Iceland, and Switzerland. However, this is not the case all over the world.

The following list* answers the question of the validity of opt-in or opt-out for around 60 countries, listed by continent. For most countries, the list also contains important information regarding the respective legal bases:

Europe

Country	Opt-in	Opt-out	Legal bases/comments
Belgium	(+)		› Law on Legal Aspects of the Services of the Information Society (Law of 11 March 2003), › Applicable to B2B and B2C
Bulgaria	(+)		› Electronic Communications Act (Art. 261, para. 1).
Denmark	(+)		
Germany	(+)		› German Civil Code (BGB) › Act Against Unfair Competition (UWG) › Telemedia Act (TMG) › Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) › Express consent required, exception with customer relationships; Section 7 para. 2 no. 3, para. 3 UWG › No differentiation between B2B or B2C
Estonia	(+)		› Electronic Communications Act › With B2B, opt-out is sufficient
Finland	(+)		› Finnish Information Society Code (Tietoyhteiskuntakaari 2014/917) (the "ISC") dated 7 November 2014 › In force since 01 January 2015 › Opt-out applies to B2B
France	(+)		› Law on Confidence in the Digital Economy (LECN) › The following applies for consumers: Opt-in necessary unless 1. Address was obtained during a purchase in the last 12 months 2. Product similarity 3. Free-of-charge and clearly understandable opt-out option › With B2B, opt-out is sufficient
Greece	(+)		› Law 3471/2006 (G.G. 133A'/28 June 2006) „Protection of privacy and personal data in the telecommunications sector"
Iceland	(+)		

Country	Opt-in	Opt-out	Legal bases/comments
Ireland	(+)		› Data Protection Act of 1998 › European Communities (Electronic › Communications Networks and Services) › (Data Protection and Privacy) Regulations › 2003 (Statutory Instrument No. 535 of 2003) › Data Protection Act of 2003 (amending Data Protection Act of 1988) › The following applies to consumers: Opt-in necessary, unless 1. Address was obtained during a purchase in the last 12 months 2. Product similarity 3. Free-of-charge and clearly understandable opt-out option › With B2B, opt-out is sufficient (Caution: Only in the case of email addresses that look as if they were business addresses and only for advertising in this business area)
Italy	(+)		› Anti-spam regulation in Section 130 of the Italian Data Protection Act, Codice in materia di protezione dei dati personali › The following applies to consumers: Opt-in necessary unless 1. Address was obtained during a purchase in the last 12 months 2. Product similarity 3. Free-of-charge and clearly understandable opt-out option

Country	Opt-in	Opt-out	Legal bases/comments
Croatia	(+)		› Zakon o elektroničkim komunikacijama, NN 73/08, 90/11, 133/12, 80/13, 71/14 „ZEK“ › In B2B sufficient opt-out (Caution: only in the case of non-automated targeting of legal entities)
Latvia	(+)		› With B2B, opt-out is sufficient
Liechtenstein	(+)		› Communication Act dated 17 March 2006 › In force since 06 June 2006
Luxembourg	(+)		
Lithuania	(+)		› Law on Electronic Communications (the „LOEC“)
Malta	(+)		
Netherlands	(+)		› Dutch Telecommunication Act; in force since 10/01/2009: The New Dutch Opt-In Law › The following applies to B2B and B2C: Opt-in necessary unless 1. Address was obtained during a purchase in the last 12 months 2. Product similarity 3. Free-of-charge and clearly understandable opt-out option
Norway	(+)		› Marketing Control Act, from 09 January 2009 › In force since 01 June 2009
Austria	(+)		› Opt-in with B2C and B2B, exception with customer relationships; Section 107 para. 2, para. 3 of the Telecommunications Act (TKG) 2003, (Amendment 2006)
Poland	(+)		
Portugal	(+)		› 2000/31/EC › Decree Law 7/2004 (Art. 22) › With B2B, opt-out is sufficient
Romania	(+)		

Country	Opt-in	Opt-out	Legal bases/comments
Slovenia	(+)		› Slovenian Electronic Communications Act (Zakon o elektronskih komunikacijah, UL RS No. 109/2012, 110/2013) (the "EKom-1") › In force since 15 January 2013 › Electronic Commerce Market Act (Zakon o elektronskem poslovanju na trgu, UL RS No. 96/2009 and 19/2015) (the "ZEPT") › With B2B, opt-out is sufficient (since 04 April 2015)
Spain	**(+)**		› Information Society Services and Electronic Commerce Act (34/2002, 11 July 2002) › Royal Decree 1720/2007 › The following applies for consumers: Opt-in necessary unless 1. Address was obtained during a purchase in the last 12 months 2. Product similarity 3. Free-of-charge and clearly understandable opt-out option
Sweden	(+)		› Swedish Marketing Act › With B2B, opt-out is sufficient
Switzerland	(+)		› Art. 3 of the Federal Law Against Unfair Competition: › Mass advertising by email is only permissible in Switzerland if the following requirements are met: 1. Prior consent from the customers 2. Indication of the correct sender 3. Information about easy and free of-charge unsubscribe option
Slovakia	(+)		› Section 62 Electronic Communications Act ("ECA") › In force since 01 November 2011
Czech Republic	(+)		› Act No. 480/2004
Ukraine	(+)		› With B2B, opt-out is sufficient

Country	Opt-in	Opt-out	Legal bases/comments
Hungary	(+)		› Act No. XLVIII of 2008 on the Basic Conditions on and Restrictions of Commercial Advertising (the "Advertising Act")
United Kingdom	(+)		› Privacy and Electronic Communications (EC Directive) Regulations 2003: › For consumers: Opt-in necessary unless 1. Address was obtained during a purchase in the last 12 months 2. Product similarity 3. Free-of-charge and clearly understandable opt-out option
Cyprus	(+)		› Section 06 of the Regulation of Electronic Communications and Postal Services Law of 2004

USA/South America/Canada

Country	Opt-in	Opt-out	Legal bases/comments
USA		(+)	› CAN-SPAM-ACT: The following points constitute the most important content of the law (Section 5): Sender must be clearly identifiable 1. Misleading subject lines are prohibited, i.e. the subject line may only inform the recipient about the true content of the email. 2. Opt-out option or unsubscribe option must be given 3. The postal address of the sender must be indicated
Argentina		(+)	› Personal Data Protection Act › There is no law solely on email marketing. Section 27 of the Personal Data Protection Act, however, contains provisions on the opt-out option with advertising emails
Brazil		(+)	› Opt-in is (still) not required, but advisable because there is the tendency to opt-in
Chile	(+)		› Law 19.628
Costa Rica	(+)		

Country	Opt-in	Opt-out	Legal bases/comments
Canada	(+)		› http://laws-lois.justice.gc.ca/eng/acts/E-1.6/index.html › since 01 July 2014: Opt-in regime, approximation to German provisions and revised anti-spam law: Canada's Anti-Spam Law (CASL); 1. Express consent from the recipient to the receipt of the advertising email before it is sent 2. No false or misleading message header (sender or subject line); 3. No change in the sending data; 4. A clearly visible or locatable "unsubscribe link;" The advertising email must contain the sender's postal address; 5. No use of email addresses that have been collected by unlawful means and
Colombia	(+)		
Mexico	(+)		
Peru	(+)		
Venezuela	(+)		› Consumer Protection Law

Africa

Country	Opt-in	Opt-out	Legal bases/comments
South Africa	(+)		

Asia/Australia

Country	Opt-in	Opt-out	Legal bases/comments
Country	Opt-in	Opt-out	› Legal bases/comments
Australia	(+)		› Spam Act 2003, always prior express consent required
Bahrain		(+)	
China	(+)		› China's Regulations on Internet Email Services 2006

Country	Opt-in	Opt-out	Legal bases/comments
Dubai		(+)	
Hong Kong	(+)		› Personal Data (Privacy) Ordinance (the "PDPO") which contains the Data Protection Principles (the "DPP") › With B2B, opt-out is sufficient
India			› Email marketing is not regulated
Indonesia	(+)		› Act No. 11 of 2008 on Electronic Information and Transaction („EIT Act")
Israel	(+)		› Section 30A of the Telecommunications Act
Japan	(+)		› „New Anti-Spam Law" 2008, close adaptation to the European principles
Malaysia	(+)		› With B2B, opt-out is sufficient
New Zealand	(+)		› Unsolicited Electronic Messages Act 2007; › Privacy Act 1993
Philippines	(+)		
Russia	(+)		
Saudi Arabia	(+)		
Singapore		(+)	› Singapore enacted the SPAM Control Act in 2007
South Korea	(+)		› Since November 2014
Turkey		(+)	
United Arab Emirates	(+)		
Vietnam	(+)		

* As of May 2016: Subsequent changes to legislation or case law in the individual countries after this date have not been taken into account in this document. Business to business contact ("B2B") in individual countries can also include only legal entities.

Note for CSA senders: The necessity of opt-in always applies in accordance with the CSA regulations in order to benefit from an optimized delivery and meet the stringent requirements of the ISPs

Authors & copy-editing

Authors

Dr. Torsten Schwarz
Owner of Absolit Consulting und
Email-Marketing-Forum.de
https://www.absolit.de

Christian Schmoll
Lawyer, g3s Lawyers
www.g3s.legal
Senior Legal Counsel, Sprinklr, Inc.
www.sprinklr.com

Lukas Bühlmann
Lawyer and Partner
Bühlmann Lawyers Inc.
http://www.br-legal.ch

Tamino Chochola
Stadler Völkel Lawyers Ldt.
www.svlaw.at

Dr. Arthur Stadler
Lawyer
Stadler Völkel Lawyers Ldt.
www.svlaw.at

Martin Bucher
Managing Director, Inxmail Ldt.
www.inxmail.de

Dr. Jens Eckhardt
Specialist lawyer for
information technology law
Data protection auditor (TÜV)
Derra, Meyer & Partner
www.derra.eu

Christian Solmecke
Lawyer and Partner
WILDE BEUGER SOLMECKE Lawyers
www.wbs-law.de

Annika Dam
Lawyer
WILDE BEUGER SOLMECKE Lawyers
www.wbs.de

Ivo A. Ivanov
Lawyer and General Corporate Counsel,
eco Association

Rosa Hafezi
Lawyer, Professional Services Division,
eco Association

Alexandra Koch-Skiba
Lawyer, Head of Complaints Office,
eco Association

Qadir Rostamzada
Marketing & Business Development,
eco Association

Copy-editing

Ivo A. Ivanov
Lawyer and General Corporate Counsel,
eco Association

Rosa Hafezi
Lawyer, Professional Services Division,
eco Association

Alexandra Koch-Skiba
Lawyer, Head of Complaints Office,
eco Association

Dr. Katharina Küchler
Lawyer, Professional Services Division,
eco Association

Sebastian Fitting
Ass. iur. Consultant Complaints Office

Peter Urlaub
Ass. iur. Consultant Complaints Office

eco
Association of the Internet Industry
Lichtstraße 43h
50825 Köln (Cologne)
Phone +49(0)221/700048-0
Fax +49(0)221/700048 - 111
info@eco.de
www.eco.de

www.certified-senders.eu

edited by