ACHIEVING LEGAL COMPLIANCE IN
MARKETING AUTOMATION & LEAD MANAGEMENT

GET READY FOR THE GDPR – NOW!

FOREWORD

Human dignity is unimpeachable. It includes the right to information self-determination. The German Federal Constitutional Court derives a particular basic right to "information self-determination" from the constitution. In principle, it is up to the individual to determine how his/her personal information is released and used. It would be inconsistent with the right to information self-determination if citizens could not know who, what, when and under what circumstances personal information is held.

With increasing volumes of data, data protection and data security are gaining greater importance, permanently. The legal collection and merging of different data is the constant concern of data protection. Compliance herewith requires special efforts on the part of all data processors, particularly in email marketing and lead management.

The EU General Data Protection Regulation EU-GD-PR comes into force on 25/5/2018. All data processors therefore have a duty to comply with the resulting rights and obligations.

Particular care must be exercised in the processing of personal data for the purpose of direct marketing.

Direct marketing is still permissible if the personal data is processed based on the consent of the person concerned, or if such processing is necessary to safeguard legitimate interests of the party responsible or a third party, and this does not outweigh the interests of the person concerned. Worth noting is the unrestricted objection right of the person concerned in cases of direct marketing, whereby individuals can entirely veto the processing of their personal data. This also includes data processing for the purpose of profiling. The person concerned should be notified of this (particular) objection right, clearly and separately from other information. Infringements of the GDPR are punishable by a substantial fine.

The person concerned should have the right to not be subjected to any decision on the assessment of personal aspects, which is based solely on automatic processing. This includes "profiling" whereby personal data as regards personal aspects of a natural person are assessed, for example regarding job performance, financial situation, health or personal interests. However, the aforementioned **decision-making should be permitted** under three conditions: if this is expressly permitted under EU law or the law of the member state relevant to the party responsible for data processing; if this is required for the conclusion or performance of a contract between the person concerned and a party responsible; or if the person concerned has granted express consent in this regard. The latter has both the right to sufficient information and the right to direct involvement, to state his/her own point of view, to explanation of the decision made based on a corresponding assessment, as well as the right to challenge the decision. These measures also should not apply to children.

Suitable mathematical or statistical procedures must be applied in profiling to ensure fair, transparent data processing, and technical and organisational measures must be taken to ensure in particular that factors that lead to incorrect personal data are corrected and the risk of error is reduced. Data must be secured in such a way that minimises potential threats to the interests and rights of the person concerned, and that prevents the person being discriminated against in any way based on his/her data.

Data processors bear a great responsibility for observing personal rights. These guidelines should help you to meet the requirements. I wish you every success!

Norbert Warga

Data Protection Auditor (TÜV), Foreman of the working group Law & Practice in the Association of German Data Protection Officers (BvD e.V.).

INTRODUCTION

The date of entry into force is 25th May 2018: the new General Data Protection Regulation shall be effective henceforth. It shall take effect on 25/05/2016 in all member states of the European Union (EU), and the transition period will soon come to an end. Companies will encounter a few changes as a result, also in the business-to-business context. The GDPR replaces the previous, national data protection legislation. If B2B companies do not want to run the risk of being penalised with a fine, they should check whether all their processes are legally compliant and adapt these if necessary. We explain the most important changes and effects in the field of lead management and email marketing. You also learn which steps you can and should implement now.

WHAT'S NEW UNDER THE GDPR?

The GDPR reforms and standardises the processes related to collection and processing of personal data. First of all, we would like to give you an overview of the fundamental changes. Therefore we have summarised the new GDPR into seven topics:

1. CONSENT TO PROCESS AND USE PERSONAL DATA

In principle, data processing is prohibited. Only where statutory authorisation exists may data be legally processed. The consent of the person concerned constitutes such statutory authorisation. But as regards consent, there are two major changes: The requirements pursuant to data protection legislation to obtain the consent of the party concerned to process and use personal data have been intensified, and the age of consent is now 16 years as standard. The latter has little impact in Germany, as the minimum age of consent remains 18 years old according to the German Civil Code. According to the GDPR, for minors the parties responsible must make "reasonable efforts" to guarantee the consent or approval of the legal representative, taking into account the available technology.

Tip: How to obtain consent for email marketing: In the online form create a declaration of consent with reference to the right of revocation (e.g. "I would like to receive the latest offers and information from the company XY by email. I can withdraw my consent at any time.") and combine this with a checkbox that is not checked in advance. Previous consents shall only remain effective if they already contain reference to the right of revocation at any time.

2. DOCUMENTATION AND REPORTING DUTY IN THE EVENT OF DATA BREACH

The compliance with data protection principles must be verifiable. Thus in the future companies must establish comprehensive documentation with the content of the directory from Article 30 of the GDPR. Exemptions shall only be granted to companies with fewer than 250 employees, provided processing of personal data only happens "occasionally". However this exemption should be applied very little in practice. Should data protection breaches occur, these must be reported to the relevant authorities within 72 hours of detection. Furthermore, the persons concerned must be informed immediately if the incident could jeopardise personal rights and freedoms. Prior to processing companies also have a duty to estimate the risks to the privacy of the persons concerned if it is likely that the data processing may involve a high risk to the parties concerned. However this regulation shall not apply to existing data processing. For example, this risk and impact assessment is required to process particularly sensitive data, such as health information. Consultation requirements come into force in the impact assessment with enforcement of the GDPR.

Tip: Preparing a directory of proceedings is particularly time-consuming, so companies should not lose any time. The working group of the German supervisory authority has meanwhile created notes and templates, which are available here: https://www.bvdnet.de/en/muster-fuer-verzeichnisse-gemaess-art-30/

3. PRIVACY BY DESIGN UND PRIVACY BY DEFAULT

Privacy by Design means that the development and operation of all hardware and software components must take all reasonable technical and organisational measures to safeguard the principles of data security and data economy. In the context of Privacy by Default, all default settings must be configured in such a way that as little personal data as possible is processed. Furthermore, only personal data required for the respective purpose may be processed.

Tip: Hardware and software must always correspond to the state-of-the-art. In the context of lead generation, please note that profiles should not simply be populated, but also reviewed as regards whether and which information can be erased from the profile, according to the respective commercial purpose.

4. EXTRATERRITORIALITY AND LEX LOCI SOLUTIONIS

The scope of the GDPR applies to all companies that processes the data of EU citizens - even if the companies are not domiciled within the EU. Thus companies such as Google or Facebook, which have until now operated in accordance with less stringent Irish data protection law, will soon have to comply with the regulations of the GDPR. Lex loci solutionis also applies: The GDPR applies if an offer is aimed at the national market within the EU or if the data processing is designed to observe the behaviour of EU citizens, for example via tracking or profiling.

5. RIGHT TO ERASURE

In the future, "parties concerned" will have the right to have their data erased from the internet. When transmitting addresses, you as a company must ensure that this request is implemented as far as possible on your part and you must inform other companies to whom you transmit addresses of any request for deletion. The party responsible must respond "immediately". The one-month deadline must be observed here, as with other requests from parties concerned such as the right to information or correction. In exceptional circumstances, this period can be extended by a further two months, whereby you must inform the party concerned about the extension period and state the reasons for this.

Tip: There are no formal requirements concerning the "requests" of the parties concerned. Requests can be made via all channels, and must then be processed within the time limit. Therefore processes must be established and responsibilities must be determined. Not least employees must be trained and briefed on incoming requests and the correct way to handle these.

6. CONTRACT DATA PROCESSING BECOMES CONTRACT PROCESSING

This change concerns almost every company, as most companies also use cloud services. According to the current German Federal Data Protection Act, contract data processing refers to data processing by order and under instruction of the principal - the principal is solely responsible. According to the new contract processing as defined in the GDPR, only one contractual relationship is required as regards data processing. It no longer matters whether the contractor is working under instruction or not. Thus in future any type of external processing of personal data on behalf of a company, such as payroll accounting, sending newsletters via cloud services or use of a calling service, will fall under the new "contract processing". This is linked to new obligations of the contract processor e.g. documentation obligations, creation of proceedings directories and reporting obligations. Previous agreements must be amended accordingly. Yet the future also brings simplification: since the GDPR no longer specifies the conclusion of separate and written contract data processing agreements. Instead electronic format shall suffice (online at the click of a mouse and together with the actual contract) for a legally compliant conclusion of contract. For example, in future the rights and obligations of contract processing shall be easily governed as part of agreements on the use of cloud services.

The suppliers of cloud services must also "offer sufficient guarantees that suitable technical and organisational measures are performed in such a way that" all data protection and data security requirements are upheld. The cloud user has a duty to monitor the fulfilment of these conditions by the cloud service. Alternatively evidence of certificates such as the standard ISO/IEC 27001 can be provided. It is therefore advisable to engage certified providers only.

Tip: A first sample for a contract processing agreement is available here:
https://www.activemind.de/en/data-protection/documents/

7. SANCTIONS

In this regard, the GDPR has correctly revised upwards, as breaches of data protection now carry substantial penalties of 10 to 20 million euro or up to four percent of the global annual turnover of the entire company, depending on which is higher. The GDPR also introduces a claim for compensation for persons concerned.

WHAT ARE THE PARTICULAR CHANGES IN EMAIL MARKETING AND LEAD MANAGEMENT?

Many of the fundamental new aspects of the GDPR concern lead management and email marketing. In the second part of our checklist, we explain the changes in detail and how these apply to you specifically as a marketing representative. We provide a specific to-do list over the next six points.

1. USE OF PERSONAL DATA FOR MARKETING

The GDPR significantly simplifies the use of personal data in marketing. The list data privilege, which only existed in this form in Germany, was abolished. The list data privilege permitted processing of legally-obtained list data without express consent - such as job title, sector description or trade name, name, title, academic degree, address, birth year. However email addresses were never included, so the list privilege did not play a major role in email marketing anyway. Instead the focus is now on commercial interests, provided the company has a legitimate interest in its use. According to GDPR, specific recitals such as direct advertising are deemed a legitimate interest. In any case under the new GDPR promotional emails may not be sent on grounds of legitimate interest, rather the advertising consent of the recipient must always be obtained.

To-do: As regards your email marketing and your lead management process, this means that you must always obtain the express consent of the party concerned. Otherwise it is prohibited to send any form of promotional emails, such as automated lead nurturing mails, follow-ups, trigger emails, interval emails or transaction emails. Postal reference to a relevant content module is also permitted: for example you may send your existing customers a reference to a landing page on a postcard. However, you must include a corresponding online form to obtain consent on the landing page. For data queries, you must observe the principles of transparency, earmarking, data economy and limited retention along your nurturing route. You should therefore precisely define the purpose of the data query at each individual stage.

2. RIGHT OF REVOCATION OF PARTIES CONCERNED

Parties concerned still have the right to object to the use of their data for email promotions at any time. This is not changed by the GDPR. The right of revocation at any time must be referenced in the online form used to obtain consent. A link, e.g. to a "data protection declaration" shall not suffice for obtaining consent.

To-do: Particularly in email marketing, this means that in addition to reference to the right of revocation in the declaration of consent, each individual email must contain an unsubscribe option (unsubscribe link in the footer).

3. DIRECTORY OF PROCESSING ACTIVITIES

The GDPR stipulates that in future the party responsible i.e. the management, rather than the data protection officer, must establish a directory of all processing activities. This task may be delegated of course, however the party responsible remains so and must monitor implementation. These are the most important aspects of the directory of proceedings: Purpose of data processing;

Description of categories of persons concerned and personal data; indication of the categories of recipients to whom the data was or will be disclosed; deadlines for the deletion of data; data transmission to non-member states, where applicable; description of the technical and organisational measures to guarantee data security.

To-do: Establish the responsibilities for your email marketing and your lead management now and start by creating the directory of proceedings. Your data protection officer can continue creating this, however the party responsible, i.e. management, shall be liable in the future.

4. CONSENT VIA CHECKBOX AND OPT-IN PROCEDURE

The processing of personal data for promotional purposes in email marketing must still be based on the consent of the party concerned. However, it is important that the voluntary nature and transparency of consent exist. Consent may be granted in writing, electronically or verbally, although verbal consent is certainly more difficult to prove. And ultimately this is crucial: as you have a duty to provide evidence under the GDPR. Accordingly you should always allow the party concerned to re-confirm its consent granted online by sending a confirmation link via email and thus performing the double-opt-in function. This confirmation email is permitted and necessary, because it merely clarifies whether the consent comes from the legitimate user of the email address. Therefore you needn't fear penalties.

To-do: In order to continue to use advertising consents that you have already obtained for email marketing, you must comply with the new data protection regulations. You should add a corresponding checkbox with a declaration of consent to your online form now and place this next to the email address field. This declaration of consent must be repeated in the data protection information on the "Data Protection" page. You must also ensure that the party concerned is informed of its right of revocation at any time in both the consent text and in the data protection information. As the consent must be verifiable, you must record each stage of the double-opt-in process in your system.

5. THE RIGHT TO DATA TRANSFER

The GDPR permits the retention of personal data in a structured, machine-readable form. Thus it grants the right of the party concerned to transfer this data to another company, for instance in the event of a change of supplier. This simplifies such a change for any party concerned, and also encourages competition between the data-driven company and the data security technologies.

To-do: Check whether your system enables data export in standard formats or via interface.

6. CREATION OF USER PROFILES AND TRACKING IN LEAD MANAGEMENT

The GDPR does not apply to anonymous data. However most email addresses refer to the recipient by name, so anonymous data processing is rarely possible in lead management.

Until now the creation of pseudonymised user profiles with opt-out solution without consent was permitted for marketing purposes, provided the user received corresponding data protection information. This regulation shall lapse without replacement with the GDPR. According to the new law, "pseudonymisation" constitutes a type of data processing in which personal data can no longer be easily assigned to a specific person, but nevertheless can be traced to persons. Pseudonymised user profiles are therefore deemed personal data under the GDPR, so in future they will only be permitted based on the consent of the party concerned. The question of whether a legitimate interest for the creation of profiles in lead management can suffice is currently completely open.

The admissibility and the framework of personalised tracking of user behaviour should be governed by a new e-privacy regulation in the future. This should come into force on 25/05/2018, but currently only exists as a draft version and is highly controversial. Accordingly any monitoring of electronic communication should be fundamentally prohibited, unless permitted by an exemption. Art. 8 E-Privacy Regulation governs the use of cookies, web beacons, etc. and permits use thereof where "necessary to measure the web audience", provided the operator of the service performs the measurement itself (First-Party-Cookies). However this is not the case in the use of cloud services, for instance, even if the measurement is ultimately only performed as part of contract processing (Third-Party-Cookies). It is yet to be confirmed whether tracking in lead management can fall within the "measurement of the web audience" exemption. Otherwise the consent of the party concerned would actually have

to be obtained. This should be possible via “technically possible and effective” browser settings according to Art. 9 E-Privacy Regulation, however the form of these is still unclear, as is their impact on the principle of Privacy by Design according to Art. 25 GDPR.

To-do: In future, those who want to be absolutely sure should obtain user consent for both creation and management of user profiles, as well as for tracking. Whether the creation of the profile can be based on legitimate interest according to the GDPR is just as open as the question of whether tracking will remain permissible in the future as an opt-out solution without extra consent under the exemption in the E-Privacy Regulation for measuring the web audience.

ACT NOW

Initially the new GDPR sounds threatening due to the high fines, but at closer inspection it also creates a uniform area within the member states of the EU. Certain points require extra effort at first, but other aspects have also been simplified. It is essential that companies act now. Follow our short checklist (see info box) and be ideally prepared when the grace period ends on 25th May 2018.

How to ready your company for the GDPR:
• Use checkboxes and double-opt-in for the consent of parties concerned. • Comply with your information obligation and update all legal texts, such as consent texts, data protection information, terms and conditions, or other information texts. • Please also note your duty to reference the right of revocation. • Take precautions as regards the documentation obligation. • Create a directory of proceedings. • Adapt your contract data processing agreements.

COMPANIES INVOLVED IN THESE GUIDELINES

ABOUT SC-NETWORKS AND EVALANCHE

SC-Networks GmbH (www.sc-networks.de) based in Starnberg is the manufacturer of Evalanche, one of the most modern, web-based email marketing automation solutions on the European market. EVALANCHE has been specifically developed for agencies and marketing departments of major corporations and offers a range of marketing automation functionalities for effective lead management. Evalanche is hosted exclusively in TÜV-certified German data centres and has been certified by TÜV Süd in functionality and data security since 2011. In 2015 SC-Networks was also certified by TÜV Hessen pursuant to ISO/IEC 27001. More than 3000 companies use Evalanche internationally.

ABOUT RESMEDIA

RESMEDIA - Attorneys for IT-IP Media (www.res-media.net) with branches in Mainz and Berlin offers companies specialist legal advice in the core fields of IT law, data protection and online marketing. The expert team comprises specialist lawyers for information technology law and commercial legal protection, who work exclusively in these fields. In particularly it specialises in providing consultation on implementation of the new EU data protection legislation, as well as establishment of new legally compliant email marketing and lead management in companies.

LEGAL NOTICE AND COMPANY DETAILS

ISSUED BY

SC-Networks GmbH

Enzianstr. 2

82319 Starnberg

www.sc-networks.com

Email: info@sc-networks.com

Managing Directors: Tobias Kuen, Martin Philipp

Register court: Munich District Court, Register number: HRB 14 65 73

TEXT & EDITORIAL

Dr. Ulrike Träger, Möller Horcher Public Relations GmbH, www.moeller-horcher.de

Sabine Heukrodt-Bauer, RESMEDIA - Attorneys for IT-IP Media, www.res-media.net

ISSUE 1

The content of these guidelines was written with the greatest amount of care. However we shall assume no liability for its accuracy, completeness and actuality.