

CRM Guide

EU General Data Protection Regulation

How CRM can support your GDPR journey



Copyright

The information contained herein may be altered without prior notice. The names and data used in the examples are fictitious, except where otherwise stated. No part of this document may be reproduced or transmitted for any purposes whatsoever without the express written consent of CAS Software AG, irrespective of the manner or the means, electronic or mechanical, by which this occurs.

© 2010 - 2018 CAS Software AG. All rights reserved.

CAS-Weg 1 - 5, 76131 Karlsruhe, Germany, www.cas-crm.com

All trademarks are the property of their respective owners.

Disclaimer

No guarantee can be made for the accuracy of the content.

Notification of errors would be appreciated.

April 2018

Content

Introduction	5
GDPR	7
What is personal data?	8
Which processes are covered?	9
Principles	10
Lawfulness of processing	11
Conditions of consent	11
Rights of the data subject	12
Data protection by technology and organization	15
Controller & data protection officer	15
Technical measures	16
In the case of personal data breach	17
Data protection impact assessment	17
Data transfers	17
Liability & sanctions	19
In practice: Preparing your CRM to conform to GDPR	20
Data collection and storage	20
Use of personal data	24
Targeted direct marketing	24
What needs to be borne in mind in relation to different forms of direct marketing?	27
Customer rights	29
Data security	30
Check list: What you should do now	33
Conclusion	39



Introduction

Welcome to today's digital world. With all its data, information and networks, the Internet offers fantastic chances and possibilities. And of course we expect to collect and share information and knowledge, communicate worldwide, be accessible 24/7 and have access to all kinds of data regardless of location. At the touch of a button we can place orders and pay for goods and services as well as conclude online transactions, some of which have wide-reaching ramifications. Many of the processes run automatically as if by magic.

However, the ease of operation also has its risks: data theft and misuse, surveillance, the 'transparent human being' and manipulation are just a few of these.

The European Union's Data Protection Regulations protect us against the risks involved in our daily data transactions, regardless of whether we act as a private person, consumer or customer.

The GDPR will apply from May 25, 2018 and has been designed to increase transparency and improve the protection of personal data.

Up until now, it has primarily been the high fines of up to 20 million Euros and the many unanswered questions which have dominated the headlines.

For businesses, however, the GDPR is also an excellent opportunity to establish good customer relationships based on trust and to develop these with focused marketing, sales and service activities orientated to customer needs.

In this guide, we explain in general terms the issues covered by the GDPR and the impact on customer management in businesses. You will also find a number of very useful tips and tricks on how to comply with legal regulations.

Please note that these tips can only be formulated in very general terms. And please keep in mind that there are further national laws and regulations which need to be taken into account concerning data privacy and data security. If you have specific questions, we recommend consulting your data protection officer or an attorney specialized in this field.

Get ready for the GDPR. We will be pleased to support you with our CRM solutions and know-how!

Your
CAS Software AG
www.cas-crm.com

in co-operation with:

Thomas Heimhalt
DATENSCHUTZ *perfect* GbR
Data protection consultant, officer and auditor
(TÜV – Technical Certification Body)



Human dignity is inviolable. The protection of natural persons with respect to the processing of personal data is a fundamental right: Every person has the right to the protection of personal data concerning him or her.¹

In order to protect these fundamental rights and in view of a European-wide harmonization, the new EU General Data Protection Regulation, GDPR, has been drawn up. It is applicable as of **May 25, 2018**.

The new regulation gives EU and EEA citizens more control over their personal data and ensures that personal data is protected throughout Europe. Thus, there will be less scope to record and use personal data for commercial purposes. Although it is not the aim of the regulation to prevent or complicate businesses transactions. On the contrary, the aim is to make the retention and use of personal data more transparent.

The GDPR applies to all businesses which sell products to European citizens and which store or process their personal data – irrespective of the location of their own main establishment ("market location principle").

Further regulations which previously applied in each EU member state might have been retained, but their terms have to conform to the GDPR.

Our expert recommends

Take the GDPR seriously and lose no time in taking the necessary measures for compliance with the provisions, since the **sanctions have been significantly increased**: Companies which breach data protection face substantial fines of up to 20 million Euros or up to four percent of the global previous year's sales of the entire group – whichever sum is higher. In addition, data subjects who have suffered material or immaterial damage have a claim to damages.

¹ According to: Article 8 (1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16 (1) of the Treaty on the Functioning of the European Union (TFEU)

Overview of the most important provisions of the GDPR

The GDPR

- ✓ lays down rules relating to the protection of natural persons with regard to the processing of personal data and the free movement of such data and
- ✓ protects the fundamental rights and freedoms of natural persons, in particular their right to protection of personal data, whereby
- ✓ the free movement of personal data in the EU shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

What is personal data?

For the purposes of the GDPR, personal data is any information relating to an identified or identifiable natural person ('data subject'), such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person – without distinguishing between personal data in a private, public or work-related environment of a person, since business relationships are always maintained by individual (natural) persons.²



Practical user tip

Within the scope of customer care and customer relationships, it is often normal for us to disclose private information such as birth dates, family status and hobbies. Before storing such data in the CRM, you should check whether this information should actually be stored or processed at all – ideally, only if it is relevant to the contract or the customer has given their permission.

² Art. 4 GDPR



Which processes are covered?

In general, data protection encompasses all processes involving personal data. The regulation meanwhile summarizes this under the term "processing".

Thus "processing" is taken to mean³:

- ✓ any operation or set of operations performed on personal data or on sets of personal data,
- ✓ whether or not by automated means
- ✓ such as
 - the collection,
 - the recording,
 - the organization,
 - the structuring,
 - the storage,
 - the adaptation or alteration,
 - the retrieval,
 - the consultation,
 - the use,
 - the disclosure by transmission, dissemination or otherwise
 - the alignment or combination,
 - the restriction,
 - the erasure or
 - the destruction

of data.

³ Art. 4 GDPR

Principles

The GDPR continues to prescribe previous data protection principles⁴ and develop them further:

Lawfulness, fairness and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

Purpose limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Should the original purpose change, this must be communicated.

Data minimization

Less is more: Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy

Personal data shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.

Storage limitation

Personal data shall be kept in a form which permits identification of the data subject for no longer than it is necessary for the purposes for which it is processed. Thereafter, the personal data is to be erased or anonymized. In this respect, the exceptions provided for under the GDPR are to be taken into account.

Integrity and confidentiality

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Compliance and accountability

The controller is responsible for and must be able to demonstrate compliance with Art. 5 (1) GDPR.

⁴Art. 5 GDPR

Lawfulness of processing

The general principle for the processing of personal data is the so-called right of permission.⁵ According to this, the processing of personal data is only admissible if the

relevant customer has given consent to the processing (or a valid exception applies under Art. 6 GDPR).

Conditions of consent

This consent is subject to certain conditions⁶, inter alia:

Burden of proof

The controller must be able to demonstrate that the data subject has consented to the processing of his or her personal data for one or more specified purposes.

Clear and distinguishable

If the written consent is given in connection with other matters, the request for consent to the processing of his or her data must be made in such a manner that it is clearly distinguishable from the other matters. Furthermore, the request must be worded in an intelligible and easily accessible form, using clear and plain language.

Right to withdraw consent

The data subject shall have the right to withdraw his or her consent at any time. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

Voluntary

Consent is only valid if the data subject gave it of their own free will. The circumstances of issue have to be taken into account to determine whether consent was given voluntarily.

Reference to purpose and processing

You have to inform the data subject of the intended purpose of processing. In some individual cases, the data subject may refuse consent or demand to know the purpose of processing, in which case you also have to inform them of the consequences of opting out.

⁵ Under Art. 6 GDPR

⁶ Art. 7 GDPR. In respect of the consent of a child in relation to information society services, further conditions need to be taken into account. The age limit of 16 years is to be observed.

Rights of the data subject

With the GDPR, individual persons receive more control over their data (rights of data subject⁷) – these include, inter alia:

Right of transparency and information

The data subject shall be informed before his or her personal data is collected and recorded. He or she shall expressly consent to having this data recorded.

Right of access

The data subject shall have the right to obtain information as to whether or not personal data concerning him or her are being processed, as well as access to this personal data and any further information with regard to: the purpose of the processing, the origin and recipient of the data, the duration of the retention of the personal data and his or her rights.

Right to rectification

The data subject shall have the right to obtain without undue delay the rectification of inaccurate personal data concerning him or her.

Right to erasure ('right to be forgotten')

The data subject may demand the immediate erasure of his or her data if, for example, the original purpose of processing the same no longer exists, if consent to the processing is withdrawn, objection is lodged against the processing or data has been unlawfully processed. Exceptions listed in the GDPR are to be observed.

Right to restriction of processing

The data subject may demand a restriction of the processing of data if this is, for example, inaccurate, is used unlawfully or if consent to the processing of the data has been withdrawn.

Right to data portability

The data subject has the right to receive any personal data concerning him or her which he or she has provided to a controller, in a structured, commonly used and machine-readable format, and has the right to transmit this data or have the same transmitted to another controller.

Right to object

The data subject may, related to differing purposes of use, object to the processing of his or her data, at any time. This objection has to occur no later than the time of first communication with the data subject. The right to object shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

⁷ Art. 12 et seq. GDPR

Notes



Data protection by technology and organization

Taking into account the state of the art, the costs of implementation as well as the likelihood and the risk for the rights and freedoms of the data subject, appropriate technical and organizational measures (TOM) are to be implemented to ensure data security.⁸ In this respect, the level of security should be commensurate with the severity of the risk.

The GDPR emphasizes the importance of technical and organizational data protection and assigns the responsibility for the same to the controller and processor.

Controller & data protection officer

The controller and the processor are to implement appropriate technical and organizational measures in order to ensure and be able to demonstrate that the processing complies with this regulation.

Companies which process personal data must designate a data protection officer in certain circumstances.⁹ This person must possess a high degree of competence in the field of data protection based on professional qualifications or comprehensive expert knowledge. Knowledge in the practical application of data protection regulations is indispensable.

Our expert recommends

Notwithstanding the involvement of competent persons, the responsibility for the implementation of data protection and data security under the GDPR remains with the company management.

⁸ Art. 5 (1) (f) and Art. 32 GDPR

⁹ Art. 37 GDPR

Technical measures

Privacy by design

Technical measures for data security and data minimization

It is easiest to comply with data protection if these measures have already been integrated into the data processing operation. This has an influence on the selection and development of data processing software and systems.

Privacy by default

Privacy by default settings

The presets and defaults should be designed to ensure that as little personal data as possible is processed. This is intended to support those users who are less technically adept and are e.g. not inclined to adjust the data protection settings according to their wishes.

Our expert recommends

An encryption or pseudonymization of data and also the technical capability of ensuring confidentiality, integrity as well as the availability and resilience of the systems can be advantageous or even necessary.



Practical user tips

- Ensure that hardware and software always correspond to the state of the art. That is, use current product versions in so far as it is reasonable.
- In connection with lead generation, do not simply enrich existing customer profiles, but consider the purpose of use in each case to determine whether any information can be erased, or has to be erased and, if so, which information has to be erased.

What you need to do in the case of personal data breach

Notification of a personal data breach

Personal data breaches must be notified to the competent supervisory authority without undue delay, no later than 72 hours after having become aware of it.¹⁰

An exception applies where the breach is unlikely to result in a risk to the personal rights and freedoms of the data subject, e.g. through suitable encryption of personal data.

Notification to the data subject

If the personal data breach is likely to result in a high risk to the personal rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

Data protection impact assessment

Impact assessments are performed where a type of processing of personal data is likely to result in a high risk to the rights and freedoms of natural persons. The controller must, prior to processing, carry out an impact assessment of the processing operations with respect to the protection of personal data.¹¹ This applies in particular in the case of new technologies, by reason of the nature, scope, context and purposes of the processing.

A data protection impact assessment is also, inter alia, necessary in cases of the processing of particularly sensitive data and of extensive video surveillance.

Data transfers

Particular attention needs to be paid to the transmission of personal data. A transmission takes place when data is communicated to third parties. In this connection, third parties are persons or bodies other than the controller. Exceptions include the data subject him or herself and also the processors.

A transmission takes place when the data is communicated to an external third party, either through the explicit sending of the same or through a commonly used customer database. This also applies in relation to a subsidiary company or any other company in the group.

A transmission of personal data to a third country is only admissible under certain conditions, such as, inter alia, individual authorization and consent of the data subject. The intention is to ensure by these means that the level of protection for natural persons guaranteed by the GDPR is not undermined.

¹⁰ Art. 33 et seq. GDPR

¹¹ Art. 35 GDPR

Notes

Liability & sanctions

High fines

It can become expensive and even endanger a company's existence: Companies which breach data protection face substantial fines which can total up to 20 million Euros or up to four percent of the global previous year's sales of the entire group – whichever sum is higher.

Liability for the damage

Any controller involved in processing personal data is liable for damage caused by processing which is not performed in compliance with data protection regulations.¹²

Right to compensation

The GDPR also introduces a claim for damages for data subjects who suffer material or immaterial damage.



Summary of practical user tips

- Document what you model in your CRM and for which purpose.
- Only store the data that you actually need – less is more!
- Define a clear authorization structure for accessing to the data.
- Document your sources, for example, where you received the data and/or information from.
- Avoid "duplicate" data records, i.e. the retention of the same data in several places.

¹² Art. 82 GDPR

In practice:

Preparing your CRM to conform to GDPR

Companies struggle to keep up with the demands of data protection laws and regulations which have been proven to be almost impossible to manage without the help of a professional CRM system. CRM solutions provide the technical requirements for the implementation of data protection in your company and offer support in connection with further organizational measures.

Data collection and storage

The challenge concerning the initial contact is the lawful recording of customer data:

- How can I record data correctly?
- What data can be stored?
- What data must be stored?
- What data cannot be stored at all?

The key words are **consent**, **data minimization** and **specified purpose**.

Only the data necessary for the correct handling of a legal transaction may be recorded and stored.

The origin of the data and, where appropriate, the details of any onward transmission of the same need to be logged and stored in order to be able to provide information as necessary.

Our expert recommends

CRM solutions **offer support** in the implementation of data protection, but are by no means a substitute for further necessary technical and, in particular, organizational measures.

Through their basic technical equipment and user-defined adaptability, the CRM solutions from CAS Software AG provide important component parts regarding **privacy by design** and **privacy by default**.

In order to obtain **consent**, the use of a form is helpful. Be sure to use clear and simple language and ensure that the consent is issued voluntarily.

The form should contain the following:

- What data will be recorded?
- For what purposes?
- Origin/source of the contact?
- what communication channel may be used?
- Reference to your company's data protection regulations, together with the contact data of the controller and, where appropriate, of the data protection officer.

Our expert recommends

When using electronic forms, the check boxes for consent must be empty. That is to say, they may not be pre-ticked.

Store the consent with the wording of the consent in your CRM, ideally in combination with (link to) the corresponding address. This will enable you at a later point in time to produce proof from the customer file that the customer consented to the storage and processing of his or her data.



Practical user tips for recording addresses

- Use **address wizards** to record addresses quickly and easily via copy and paste – this eliminates typing errors.
- **Input aids**, automatic completion and consistency checks ensure that addresses are recorded in full and correctly.
- Create separate **fields** for all the information to be recorded insofar as this is not already provided in your CRM, e.g. for the address origin (source of the contact), date (date of initial contact), initial contact by (staff member), purpose (specified purpose), permitted communication channel (channel), erasure deadline/erasure date.
- With the use of **mandatory fields** you ensure that your staff record in full all relevant and obligatory information relating to a customer.
- In line with data minimization, only the data which is absolutely necessary should be collected and stored. Do not define any mandatory fields for data which is not necessary.
- Use the flexibility of your CRM solution in order to present the information concerning each contact in a clearly arranged manner, where appropriate, in various registers, and thus facilitate quick and easy data entry.
- Where a CRM solution with a **questionnaire module** is used, a questionnaire can also guide the user in recording addresses or in clarifying the contact wishes.
- If the questionnaire module also offers **online questionnaires**, you can also have this completed by the customer him/herself. Accordingly, it is his or her decision which data is recorded and for which purpose it may be used.
- Ideally, replies can be transferred directly from the questionnaire to the address data record by means of the **field connection**. Unnecessary work and possible transcription errors are thereby avoided.

Notes



Use of personal data

Targeted direct marketing

After an address has been correctly recorded and stored, the next step is to address the customer directly.

The customer may only be contacted

- if he or she has granted his or her consent,
- via the permitted communication channel and
- for the permitted purpose.

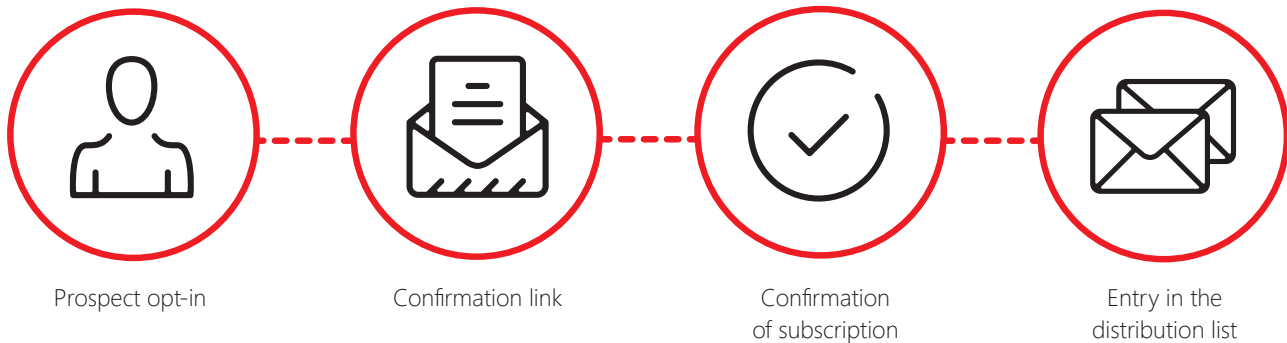
In order to obtain permission for an appropriate customer contact, his or her **consent** (opt-in) is prescribed, in particular in relation to direct marketing.

In order to avoid aggravation and misunderstandings, the simple **opt-in** process is replaced by the **double-opt-in** process in which the interested party has to confirm his or her subscription e.g. to a newsletter, in a second step. For this purpose, an e-mail will be sent to the registered e-mail contact address together with a request for confirmation. Only after the confirmation has arrived the registration becomes effective.

How to obtain consent for e-mail marketing

To comply with the data protection provisions you have to ensure that you receive explicit consent. Using the **double-opt-in** is a good way to ensure compliance and secure consent in your e-mail marketing.

1. Formulate a clear and concise declaration of consent in the online form. It should contain the following points:
 - Purpose of use, e.g. topics addressed in the newsletter
 - Communication channel (e-mail, telephone, fax, SMS, letter)
 - Contact data fields depending on the communication channel - mandatory fields should only be used for essential contact data, e.g. mail address for e-mail marketing
 - You should include a reference to the Data Protection Regulations, either in the body of the text or as a link
 - You should also include a reference to the right of withdrawal: Reminding recipients that they can withdraw consent at any time
 - Consent checkbox: Once the recipient marks the checkbox and submits the form they consent to the first step, i.e. the advertising (opt-in)
2. Send the prospect an e-mail to the e-mail address they entered in the online form, with which they can confirm their consent. The easiest way to do this is to include a confirmation link in the e-mail.
Note: the confirmation e-mail cannot contain any advertising or offers.
3. By clicking the link in the opt-in confirmation request e-mail the prospect confirms their consent to receiving e-mail advertising.





What needs to be borne in mind in relation to different forms of direct marketing?

Advertising by e-mail

Using the opt-in process the consent of the customer is usually required, in contrast to the opt-out arrangement.

We recommend you to use the double-opt-in process which offers additional protection against misuse.

With each mailing, the attention of the addressee is to be drawn to his or her right of withdrawal of his or her consent and it must be shown how he or she can exercise this right of withdrawal.

In short: Each advertising mail must contain a possibility to unsubscribe, ideally via an unsubscribe link.

Advertising by telephone

For direct marketing by telephone we recommend the opt-in arrangement. The telephone number must always be displayed.

Advertising by fax

In the case of advertising by fax, the necessity of consent applies.

Postal Mailings

Marketing through the post is the traditional and oldest form of direct marketing. Before you can use personal data for postal marketing, you must tell customers (or potential customers) that you intend to use their data for this purpose and give them an opportunity to refuse such use. You can contact the addressees as long as they have not objected.

If any customer objects, you may not use their personal data to directly market them. The individual may withdraw their consent to direct marketing at any time.

Our expert recommends

First of all, ask your customers and potential customers already during the initial contact for their consent to receive mailings and newsletters, and have this confirmed, e.g. in accordance with the double-opt-in process. Bear in mind also the duties of documentation and the burden of proof under the GDPR.



Practical user tips for selective customer contact

- You can **obtain** consent by simple means using the **questionnaire module** in your CRM solution.
- A positively completed questionnaire serves as legitimization for direct marketing. Archive this consent in your CRM, ideally in **combination** with (link to) the corresponding address data record so that you are at all times in a position to provide proof that the consent has been granted.
- Separate address fields for consent and for the permitted/desired communication channel facilitate the selection of addressees and the creation of mailing lists.
- With a marketing module in your CRM solution, you generally have comprehensive possibilities to plan, implement and evaluate multilevel campaigns: Using mailing lists and campaigns, you can address your customers according to their wishes. The customers are automatically allocated to the individual communication channel of post, e-mail etc., based on **fields** such as 'Preferred contact method' or 'Permitted contact method'. If a certain contact channel is not permitted, the CRM will ideally draw attention to this fact.
- E-mail marketing tools also offer convenient and effective possibilities of customer contact. In interaction with the CRM solution, the addresses are provided from the CRM, and the personalized mailing is professionally implemented. Following this, subscriptions/unsubscriptions and also bounces are transmitted back into the CRM, so that the addresses, together with their consents and mailing lists, remain correspondingly up to date.
- Ensure that an **unsubscribe link** is contained in each e-mail marketing campaign.
- Create the role of a designated person responsible for address and data management in your company.

Customer rights

The rights of the data subjects are expressly strengthened in the GDPR. For instance, a customer has the right to have his or her data rectified, blocked or erased. In addition, he or she has the right to receive information free of charge about all personal information stored – under the right of data portability, also in a structured, commonly used and machine-readable format.



Practical user tips to comply with the rights of customers

- CRM is a great, almost indispensable support in documenting customer data and in the recording, processing and use of the same. A **journal function** can ensure that all changes to the address data record are seamlessly logged. In the customer dossier you can check, when the address e.g. was added to which mailing lists, which contacts and interactions have taken place and which information was sent and when.
- Using the dossier you can track and record which data has been forwarded to whom and ensure that you have the necessary consent for the transmission of this data.
- With a **reports tool**, reports can be created at the press of a button. They list all the data stored in relation to a person. This enables you to comply with any person's right to information seamlessly and without great expense.

Our expert recommends

The duty to provide information, presents companies with major challenges, in particular when data is stored in separate places and first needs to be gathered together. In this case, efficient action is essential to respond to enquiries quickly and in an uncomplicated manner. The increased awareness of data protection issues may lead to an increase in the number of inquiries.

-
- Most CRM solutions also offer **export functions**, ideally in various file formats. This enables you to comply with a person's right to data portability.
 - If data needs to be rectified or completed, a **questionnaire module** with an online questionnaire may prove to be useful.
 - The data subject has the right to demand the rectification, erasure and/or blockage of his or her address. This person may forbid the dissemination and transfer of his or her own address. Comply with your customers' wishes by setting **corresponding tags** in the CRM.

Data security

The security of customer data includes

- protection against data theft,
- protection against misuse,
- protection against unauthorized access.

The aims of a software tool include the simplification of the work for users. For this purpose, the software offers many useful functions. However, if the functions are improperly used, they may also cause problems.

Particularly in sensitive areas, it is important to offer efficient and customizable functions.

Security mechanisms in CRM solutions help to prevent data being misappropriated, in particular personal address data from being exported or transferred. For instance, individual functions such as export, reports and mobile data use, should be linked to special user rights which the administrator may completely close down or only release specifically for individual employees.

Set against this, there is nevertheless a desire for

- flexible access to data via interfaces while traveling,
- efficient working through convenient functions such as drag & drop and
- adaptability of the system.

Each company has to find its own optimal solution between these two contrary aims. Complete or 100% protection against data theft and/or misuse is technically not possible – however, it can be significantly impeded.

Our expert recommends

Have your staff sign a **data protection declaration** which makes it clear that the personal data is the property of the company and may only be used for defined applications and for specific purposes in a specific scope.

In addition to the technical and organizational measures, define detailed instructions and **process descriptions** for your staff, and train them in preparing, altering and erasing data records. Also communicate to your staff the relevance of the above topics.



Practical user tips on data security

- The guiding principle for CRM solutions and also for all other systems is: With **passwords and guidelines** you create an effective method of access control.
- Create clear **rights structures**, and ensure compliance with the same. The more sophisticated and developed the rights system of your CRM solution is, the better.
- Possible rights levels:
 - Rights for user groups, e.g. for departments and hierarchy levels
 - Rights to modules, e.g. report and marketing
 - Rights for functions, e.g. import and export and also the mobile use of data
 - Individual rights to data record types, e.g. sales opportunities
 - Individual rights at a field level, e.g. for personnel data
 - Individual rights to specific data records, e.g. confidential appointments
 - Various rights, from the right to read through to full rights
- A detailed documentation of a rights concept ensures clarity and transparency.
- In order to keep the administration expenditure within limits, it should be possible to change the rights of several users at the same time and for all privilege settings to be adopted in duplication processes.
- It should also be possible to set a specific right to erase data records so that no data can be permanently erased willfully or by mistake. In order to prevent mistakes, it is recommended to have a two-phase process displayed above the trash bin when data is to be erased.
- Look for quality seals such as '**Software made in Germany**' and in particular '**Software hosted in Germany**'. In particular software solutions bearing the latter certificate are not only characterized by top quality and future viability, but are also hosted in a data center in Germany subject to German data protection law.¹³

¹³ The quality seals 'Software made in Germany' and 'Software hosted in Germany' are awarded by the Federal Association IT for Mediumsized Enterprises (BITMi e.V.), www.software-made-in-germany.org

Notes

Check list:

What you should do now



Create awareness

Creating awareness for data protection within your company: Everyone within your organisation or company needs to know about the new provisions and the guidelines of the EU GDPR.

Business owners need to ensure they have given all employees clear guidance on the regulations and procedures concerning their respective areas of responsibility and enforce adherence for due diligence. This ensures that data protection is observed uniformly throughout your company.



Designate a data protection officer and involve them closely in the implementation

If, as a rule, at least nine members of staff are concerned with the processing of personal data, you are required to formally designate a data protection officer.

The data protection officer controls and regulates the implementation of the data protection provisions in your company. It is most important that someone in your organisation takes proper responsibility for your data protection compliance and has the knowledge, support and authority to carry out their role effectively.

Any person in the company can be appointed data protection officer if he or she possesses the necessary professional competence in data protection or acquires it through training and/or further education programs.



Auditing your personal data

You should review any personal data you already have in your company and document the following:

- The type of personal data you have stored – this includes both customer data and also staff data,
- the source of the data,
- the purpose for which the data was collected and stored,
- as well as the location of the stored data and details on how long the data is to be stored.

If necessary, perform a data clean up in which only that data is retained which is necessary for the specified purposes. Other data should be erased.



Creating a directory of procedures / list of processing activities

If not already in place, set up a directory of procedures in the form of a table and provide it to the supervising authorities. The table should list which data has been collected in your company as well as when, how and why. Please note, it is important that you include internal personnel data and customer data.

Each department within your company should create a table containing procedural descriptions that address the following topics:

- Type or category of data (e.g. address data, CVs, account data etc.)
- Purpose of the data processing (e.g. recruitment management, marketing etc.)
- Date on which the data was collected
- Information provided to the data subject concerning the collection, storage and processing of his/her data
- Data subject's consent
- Recipient/Controller (who has access to the data)
- Erasure and erasure deadlines
- Procedure for providing information to the data subject and content of this information
- Conversion of data to another format for the purpose of data portability

- Data storage period (if the data is not being used)
- Technical and organizational measures related to data protection (inter alia, pseudonymization)
- Transfer of data (e.g. to third countries)

In addition, you should document the entire route of personal data – from its collection to its storage through to the use of the data.

Define your processes and create a process manual

Document all procedures in your company connected with data processing and adapt them, if necessary, to conform with the data protection guidelines.

Typically, these processes include, among other things:

- The manner in which inquiries are handled within the scope of data subject rights including duties to provide information,
- the documentation procedure and the duty to demonstrate compliance with the data processing requirements,
- and also the notification of data protection breaches. In this case, you should consider both the technical processing and also the behavior of your staff.

Data protection impact assessment

Any person who works with particularly sensitive data must handle it with exceptional care and, in certain circumstances, perform a so-called data protection impact assessment. It serves your company as a precautionary measure which you can use to assess any possible risks to the personal rights of the data subjects while processing their data. Additionally, it allows you to plan for and implement appropriate protective measures.

This is especially the case for those companies which process sensitive information such as e.g. information concerning health, finances, ethnic affinity and political affiliation.

Consent

Check how your company obtains, stores and manages data processing consent. This extends to any procedures and forms used. If the processes currently implemented do not conform with the data protection provisions, you should adapt your procedures and the respective forms. If necessary, renew any existing consents.

Plan, check and document TOMs

If you are not already using them, you should introduce technical and organizational measures (TOMs) into your company to comply with the data protection provisions. Apart from technical measures 'privacy by design' and 'privacy by default', appropriate measures include the pseudonymization and encryption of data and also the introduction of strict authorization structures to access data.

Notes



Conclusion

In this guide, we have considered the data protection provisions which have a particular impact on customer relationship management. We have also tried to demonstrate how you can use CRM to satisfy the important demands of the GDPR and implement further laws.

Address the topic of data protection in depth, check your existing data and also all processes concerning personal customer data. Use these to devise appropriate data protection measures which serve the individual needs of your company.

Talk to your data protection officer and draw up a manual for data protection in your company.

Companies without CRM will find it difficult to comply with data protection. Using a CRM solution from CAS Software AG will give you a definite advantage in meeting the regulations.

In this way, you accept the challenge of data protection and take advantage of the opportunities it offers. We wish you every success and hope that your customer relationships continue to flourish.

Faithfully yours
CAS Software AG
www.cas.de

In co-operation with:

Thomas Heimhalt
DATENSCHUTZ *perfect* GbR
Data protection consultant, officer and auditor (TÜV)
www.datenschutz-perfect.de

Contact

CAS Software AG
CAS-Weg 1-5
76131 Karlsruhe, Germany
Telephone: +49 721 9638-188
E-mail: crm@cas.de
www.cas-crm.com

