SUGARCRM

Getting ready for GDPR

A practical guide to better customer relationship management

A note from the author

Anthropologists claim that human societies all share a trait that guides our social thinking: reciprocity or “give-to-get” for short. Basically, it’s trading something of value for something else of value.

The private information that belongs to me as an individual is obviously of such great value that it deserves government protection. If data about my behaviour and my needs is being collected and used without my permission, I might worry about potential abuse thereof.

But if an organisation tells me not only what data it’s collecting on me but why they want to collect it and how its use will positively benefit me as an individual, then I will be more inclined to agree to it, if I see the value.

The General Data Protection Regulation (GDPR) is the new EU law for the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

No matter if you are a marketing, sales or support executive who deals with customer data, a Data Protection Officer, an executive with liability for compliance or just someone who wants to use customer data sensibly, you must have a plan in place or risk falling foul of the law.

This guide offers an introduction to GDPR and what it means for customer relationship management (CRM). It also explains why and how a modern CRM system can provide the perfect infrastructure for executing and consolidating GDPR efforts with respect to managing not only customer but all other relevant data.

Phil Winters

About the author

Phil Winters’ passionate focus on the customer over more than three decades has earned him international recognition as an expert in customer experience, customer journey mapping and customer intelligence. He defines new approaches that help organisations to raise their customer value and increase loyalty by delivering outstanding customer experience.

www.ciagenda.com

Introducing GDPR

Why new rules will revolutionise Customer Relationship Management

On April 27, 2016 the EU passed the world's strongest and most far-reaching law aimed at strengthening citizens' fundamental rights in the digital age. The regulation also tries to facilitate business best practices by unifying rules for companies operating within the EU Digital Single Market.

This new, 88-page General Data Protection Regulation (GDPR) is something that EU member states voted for unanimously: one law for the entire region. And it will be enforceable as of May 25, 2018.

Before this new legislation, it was up to individual countries to decide how to implement existing EU laws and recommendations, which added to complexity for businesses operating in multiple countries.

The GDPR not only applies to any company, organisation or body established in the EU who process personal data but also to any company, organisation or body established outside the EU if they target individuals residing in the EU.

The GDPR seeks to establish a modern and harmonised data protection framework across the EU. Some aspects make for quite alarming reading – particularly the parts about the sky-high fines that can be imposed on persons and organisations in breach of compliance: €20 million or 4% of a company's global turnover, whichever is the highest.

Many aspects of the law require careful evaluation and action by organisations and their legal teams and there are many recommendations on how to move forward if you are a new organisation starting from scratch. But, the majority of us will already have systems and processes in place that contain personal data – so the green field approach will not be suitable.

Concrete suggestions are required about how to get existing systems and processes compliant by May 25, 2018 as well as how to proceed thereafter. There are a few overriding themes in the GDPR that centre on the collection and usage as well as ability to report and act on personal data – this is where a good CRM System can play a critical role.

Need to know

One of the key questions people ask when it comes to GDPR is: "What is the difference between a controller and a processor?" The answer is as follows...

A controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. If a person or organisation initiated the collection of personal data either directly or indirectly, they are the controller. Examples of this are running a website, collecting customer data for a marketing campaign, interacting with customers in a structured way and providing downloads in exchange for registration.

A processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. If a person or organisation provides a service or system for their clients that has customers' personal data contained within it, they are the processor. Examples of this are a market research, marketing agency or a third-party service provider handling customer data on a company's behalf.

The bigger picture

Before considering how a CRM system can be used to support overall GDPR activities, it is important to understand that a CRM system is just one of the IT systems that will be processing personal data.

A data controller has to ensure that data protection by design and default is applied to all those IT systems. This means the data controller will need to put into place appropriate technical and organisational measures.

These measures must be designed to implement data-protection principles in an effective manner and to integrate any necessary safeguards into the processing to meet the requirements of GDPR and protect the rights of data subjects.

The controller must also take care to ensure that, by default, only personal data necessary for each specific purpose of the processing are used.

The inner workings of GDPR

The nuts and bolts of the new legislation explained

Here is an opportunity to take an in-depth look at some of the requirements of GDPR in the context of a CRM system. It examines important capabilities the system must provide to support GDPR compliance around capturing data and processing.

For ease of reference, the relevant article is included. And remember, there is a requirement to respond "without undue delay".

Article 6: Lawfulness of processing
Provide the capability to:
• Explicitly capture and associate one or more permissions with an individual record as per Article 7 defining conditions of consent.
• Alternately to associate a record of lawful processing because of a legal or contractual obligation or a justification.

Article 9: Processing of special categories of personal data.
Provide the capability to:
• Mark any identified special category personal data and to restrict access and use of such data.
• Associate a record of lawful processing based on one of the 10 exceptions listed in Article 9

Article 12: Transparent information, communication and modalities for the exercise of the rights of the data subject
• For any requests that data subjects have regarding personal data, the CRM should provide capabilities to provide the information in an easily understandable format.
• The CRM should document the fact that this request has been made as well as executed.

Article 16: Right to rectification
• If a data subject requests that inaccurate information contained be corrected and if that information is contained in the CRM system, then the controller needs to correct this data and provide a record that this process has occurred.
• Capabilities to notify the data subject that the inaccurate information has been corrected in the CRM.

Article 17: Right to erasure
• If a data subject requires data to be erased, then the CRM must be able to do the following:
i. If valid, erase the data and send a confirmation to the data subject and attach a data entry to the data subject's record that this has occurred
ii. If invalid, then send a notification to the data subject and attach a data entry to the EU resident's record that this has not occurred.

Article 18: Right to restriction
• If a data subject invokes Article 16 or 17 where the CRM is involved and the request requires time for investigation before a decision can be made, then the CRM should provide capabilities that temporarily removes that information from use by authorised individuals.
• The data subject should be notified and a record of that notification should be captured.

Article 19: Notification obligation
• If any rectification or erasure of personal data or restriction of processing was carried out in accordance with the above articles, then the controller must notify each recipient to whom the personal data have been disclosed of the exact rectification, erasure or restriction. The CRM system should provide the capability to notify these recipients.
• The controller shall also inform the data subject about those recipients if the data subject requests it. The fact that the EU resident has requested this should be acknowledged and tracked by the CRM.

Article 20: Right to portability
• A data subject has the right to have their personal data transferred to another provider. While the CRM system may not be the primary source of this information (telephone numbers, health records, bank transfer details, etc.), it might be used to consolidate this data. If this is the case, then the CRM system should provide the capability to provide the required information in a form that can be transferred to an alternate provider.
• The data subject should be notified and a record of that notification should be captured.

Article 21: Right to object
• If the CRM uses any form of automated decision making (such as next best product, next best offer, risk assessment, potential for purchase, etc. for any type of profiling purposes) that uses personal data and the data subject objects to that information being used, then the CRM system should have the capability to eliminate that personal data being used for the automated decision making.
• The fact that the data subject has requested this should be acknowledged and tracked by the CRM.

Article 25: Ability to limit access to personal data.
Provide the capability to:
• Identify and mark exactly what personal data is contained within the CRM.
• Set up specific access groups of individuals and other IT systems on a need-to-process/need-to-know basis.• Ensure only the minimum amount of personal data is actually surfaced to each group of individuals or other IT systems to complete required tasks.
• Generate reports showing which personal data was accessible to which groups.

Article 34: Notification of a data breach
• When a personal data breach is likely to result in a high risk to the rights and freedoms of the data subject, the controller shall communicate the personal data breach to the data subject without undue delay.
• The fact that a breach has happened should be acknowledged and tracked by the CRM.

Opportunity knocks

Why having a CRM system at the heart of your organisation could provide a competitive advantage

Until now, we have spoken of the capabilities a modern CRM system must provide to support GDPR compliance activities. But there will be many other systems and processes that contain personal data and therefore you will need to consolidate all that information in one place. This is to avoid duplication of efforts when responding to any data subject's legal requests and to provide them with one coherent and consolidated response. That is where the modern CRM comes in.

Think of what a modern CRM system provides above and beyond simply capturing data: lead qualification processes, opportunity tracking systems, case resolution scripts, yearly account plans and even customer journey maps. This means mechanisms for implementing, automating and tracking processes and standard procedures, as well as for surfacing those processes to users in different forms are already in place. Like blood flowing through the heart at the centre of a body, data runs through a CRM system, powering multiple areas of the business.

The CRM system infrastructure is perfect for satisfying many GDPR requirements, not only of its own use of personal data but also for consolidating all the other IT systems' compliance to GDPR requirements, all in one place. And that can help with one of the most important points as outlined by Article 12: providing transparent information, communication and methods for the controller and processor to support the data subject's rights both initially as well as on an ongoing basis.

A good CRM system can help with both one-time as well as ongoing requirements across the organisation to support GDPR. Think 'information reciprocity.' This is exactly what you need to satisfy the more detailed requirements around data consent.

Going back to Marketing 101, what's the difference between a new and an existing customer? Data! The common understanding is that a new customer costs seven times more to acquire and keep than an existing one.

Keeping this basic premise in mind, businesses should consider revisiting their Data Privacy Policy. Because, if it were actually attractive, interesting and understandable, and if it presented the topic as a differentiating factor, customers would clearly see the benefit to themselves. Instead of grudgingly satisfying the new law, businesses should look at the opportunities and benefits that the rewriting of permission language can bring.

Alternately, when processing personal data because of a permissible reason given in Article 6, be prepared to have processes in place to explain that to the data subject. Since there is a need to capture and store that procedure anyway, what better a place to do that than in a CRM system? The transactions of exactly what was surfaced and how the permissions were obtained (along with copies of the documents and date/time stamps) should be linked within the CRM to each specific individual.

This really reaches the heart of the matter. By embracing the use of a CRM system to comply with GDPR, it becomes possible to effectively manage the processes and procedures that will become a necessary part of running a business day-to-day. This should be seen as a huge, positive opportunity to provide customers with a better user experience.

Tell your customers what you're planning to do with their data and why: To help them find what they're looking for; make better recommendations; notify them of important matters (such as payments due, software updates, health notifications); and to give them the best price or special offers. The better you present it, the more likely they are to see the value and reciprocate by granting you the permission you seek.

Getting ahead

A step-by-step guide to implementing a successful CRM system that supports GDPR compliance

Before May 25, 2018, businesses will need to carry out a number of activities to investigate the degree of compliance of existing systems and processes. In addition, they will want to ensure that those existing processes – as well as any new ones – support GDPR compliance in an ongoing way.

1 Personal data audit

The first thing on your GDPR checklist should be a personal data audit. This entails identifying all systems and processes throughout the organisation (as well as your processors' and their systems that do this for you) to identify which personal data on data subjects is collected and stored and how it is used (such as profiling). You will want to document the exact nature of that data, how it was collected, how it is used and whether the data ages and gets removed when no longer relevant.

If you have an existing CRM system, this will obviously be one of those systems. But a typical organisation will have collected personal data in many places such as marketing systems, including marketing automation and online systems, sales and service systems, financial systems that involve payment and/or risk, warranty or support systems, and other operational transactional systems.

You will also need to identify any systems that contain those special categories of personal data and how – if at all – that data is being used. This is related to Article 9 and the processing of special categories of personal data.

2 Automatic profiling audit

One important topic in the audit will be identifying where automatic profiling occurs. Automatic profiling means rules and algorithms, data mining, machine learning and statistics that take decisions without the intervention of a human being.

Automatic profiling may be baked into campaign management, marketing automation, CMS and web systems, omni-channel marketing, analytics and predictive analytics: anywhere that personal data is used to figure out a model for predicting an outcome or for categorising an individual and where that information is then used automatically to take an action.

Since a data subject has the right to know about automatic profiling and to specify that they do not want it, it is important that you have the information captured in your audit. Having a clear description of each system or process in a standard format, along with a main internal contact for any detailed questions, is already a good start on the road to being GDPR compliant. It helps you not only to document the "now" but provides a basis for the ongoing activities you will need to perform to stay compliant as new systems and processes are added.

3 Per-data-subject identification

Not all systems and processes containing personal data will apply to all data subjects, so the next step is to extract a list of all data subjects who are affected by a given system or process. This does not need to be a huge, multi-year IT project, but is something that can be carried out once, either internally or with external help using existing tools.

These lists are then combined so that you can identify – for any specific data subject– exactly which processes and systems use personal data and how. For companies that have unique identifiers for individuals across all their systems, this will be straightforward. But even so, modern fuzzy matching is so good these days as to get a relatively accurate picture fairly quickly.

Why is this important? Because of all the Articles that give rights to a data subject, an individual. Those individuals are not interested in the organisational strategy surrounding GDPR but instead want to know specifically what affects them personally and any preliminary work you can do now to make the task of surfacing this information to the data subject will be time well invested for later.

This is where a modern CRM can be of great value, because if you have that list of processing per data subject you can attach a record of all of that information to each data subject in the CRM system.

Although this is initially a onetime task, you can use it as a basis for ongoing compliance, for example when processing changes or new data subjects are added to one or more systems. With the processes in place in your CRM, this can become a fully automated process.

4 Obtaining Consent or Documenting Lawful Usage

One special case of documentation will be around one of the strongest concepts in the new law: Article 6 and either gaining permission to capture and process data in specific ways or alternately documenting which subsection of Article 6 applies for not requiring consent.

While most people are accustomed to 'opt-in' arrangements via cookies, the requirements of Article 6 go much further by requiring companies to be extremely clear about what they are collecting, how they are processing the data, and where they intend to use it.

While the actual wordings for gaining consent are beyond the scope of this article, it is very clear that most businesses will have to review this carefully. They will also have to do a much better job documenting the mechanisms used to surface and capture the responses. In more complex organisations, there may actually be multiple explanations and permissions that need to be surfaced and captured.

5 Satisfying Data Subject Requests

If you have done as suggested above, you have already captured all relevant personal data and related topics. You now need a process of capturing the request, consolidating required information and taking appropriate steps when required, creating a confirmation for the data subject, having that response manually authorised by an appropriate person internally, on approval sending the relevant confirmation as well as logging each step of the process.

In a good CRM system, this will be a series of tasks and subtasks that will be well defined and that can be associated and executed quickly to any specific data subject request.

6 Internal Processes

In the same way, you will have certain internal processes that you will want to set up and occasionally execute, either manually for one data subject or automatically for a group of data subjects.

Processes might include one for Article 34: notification of a severe Data Breach or one for gaining consent for an extended use of personal data (possibly to be able to give the data subject – your customer – a better offer).

Introducing the Sugar Data Privacy Module

If a CRM system is already in place or planned, it will be a key source of personal data and needs to be incorporated into any GDPR compliance activity. A well-designed CRM platform will contain out-of-the-box functionality to help teams implement best practices for data privacy.

SugarCRM is fully committed to supporting customers with CRM software that supports GDPR compliance. Since the Sugar Spring '18 /and Sugar 8.0 releases, SugarCRM provides a dedicated Data Privacy Module. Here are its key features:

Managing Consent
Functionality to capture and record consent, as well as support the withdrawal of consent. All changes are captured and tracked.

Opt-In/Opt-Out Policy
Management of required 'opt-out' policies and capturing 'opt-ins' for activities involving direct connections from Sugar via email. In addition, clear indications of 'opt out' are surfaced so that legitimate contractual emails can still be sent when required.

Data Minimisation
Restriction of personal data usage for specific purposes and groups of users. Sugar allows for access to personal data to be restricted if required, depending on the user's role.

Right to Access
Supports the logging of all data, including source details of that data if they come from another system. Comprehensive summary reports can be created per data subject as required.

Right to Erase (Right to be Forgotten)
Erasure of information requested by a data subject including the documentation of that erasure activity. A record of the fields of information is kept along with the requesting individual. The actual contents of those fields is securely deleted and not available in any form in the future.

Right to Rectify
Logging of changes to the personal data based on the data subject's request.

Right to Object to Processing
Marking specific fields of personal data (and logging thereof) that the data subject does not want used.

GDPR Transaction Logging
All transactions associated with the above GDPR tasks are logged.

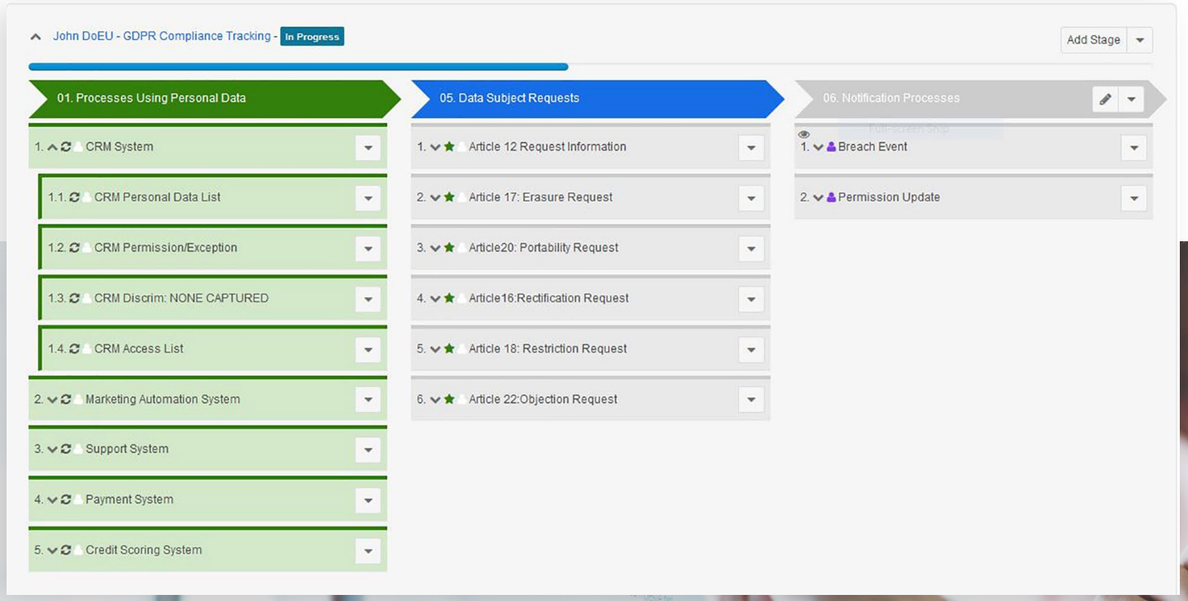
GDPR Reporting
All data processed in the above activities is available for compliance reporting.

Using CRM for orchestrating GDPR compliance

A CRM will be just one of many systems in a business that contain data impacted by GDPR. An Enterprise Resource Planning (ERP), marketing automation or campaign management system, support or ticketing system, or even HR system, could all contain personal data. These will all require the same capabilities to manage data subject requests and document changes for GDPR compliance activities.

To make it easier for you to orchestrate all your GDPR compliance requirements across multiple tools and platforms, SugarCRM also provides an optional visual GDPR Compliance Tracking tool that supports the implementation of a solid GDPR compliance programme. The visual process is fully flexible, allowing modification or expansion of each step or task to suit the unique needs of individual organisations.

Visit **www.sugarcrm.com/resources** to see a video demonstrating how this works.



The compliance checklist

There is no doubt that an approach involving a modern CRM can greatly reduce the stress and work required to comply with GDPR, not only before May 25, 2018, but for the ongoing process as well. The potential for actually improving the customer experience while doing so means this approach should be considered strongly.

To summarise, here is an eight-point GDPR compliance checklist:

1. Perform a Personal Data Audit
2. Create a per-data-subject list of relevant processes
3. Document Consent or Lawful Usage
4. Initialise your CRM for capturing and documenting GDPR Processes
5. Transfer the first three points into your CRM
6. Implement an ongoing process for the first three points to be updated in your CRM
7. Define processes for data-subject requests
8. Establish Internal Notification/Change Processes

The jargon buster

An A-Z of GDPR

Consent
Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Controller
The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. In general, if you initiated the collection of personal data either directly or indirectly, then your organisation is the 'controller' and liable under GDPR. Running a website, collecting customer data for a marketing campaign, interacting with your customers in a structured way, providing downloads in exchange for registration – all of these would be examples of your organisation collecting data and acting as a 'controller'.

Personal data
Any information relating to an identified or identifiable natural person ('data subject'): an identifiable natural person is one who can be identified, directly or indirectly, by a name, an identification number, location data, an online identifier or to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. If you are a 'controller' or 'processor' of personal data in an EU country, GDPR will apply to you for any data subject, regardless of their physical location. If you are a 'controller' or 'processor' anywhere in the world and you process personal data of a data subject that is a resident in the EU, then GDPR will apply to you. There is no distinction between Business to Consumer (B2C) and Business to Business (B2B) personal data in this respect.

Personal data breach
A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing
Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. That will cover all IT systems that contain personal data, regardless of whether those systems are on your own site, in a cloud or provided by a processor.

Processor
A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. If you provide a service or system for your clients that has their customers' personal data contained in it, then you are a processor and are subject to the law. Examples of this are a market research, marketing agency or a third-party service provider handling customer data on a company's behalf. A controller will want to work closely with a processor (and may demand not only good GDPR compliance documentation but also liability responsibilities) to ensure they and the processor are compliant with GDPR. The personal data the processor has about their client contacts makes them the 'controller' of that data.

Profiling
Any form of automated processing of personal data consisting of the use of personal data relating to a natural person, in particular to analyse or predict that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. If you are using any sort of rules like machine learning, advanced analytics or AI in any of your IT systems and if those use personal data, then there is profiling being performed.

Recipient
A natural or legal person, public authority, agency or another body, to which the personal data is disclosed.

Regulation
A legal act of the European Union which, on enactment becomes enforceable as law in all member states simultaneously. This is from May 25th, 2018 after a two-year transition period and, unlike a directive, it does not require any enabling legislation to be passed by national governments and is thus directly binding and applicable. So this is a law that could affect you. Whether your organisation is affected by this regulation depends on whether you process 'personal data'.

Restriction of processing
The marking of stored personal data with the aim of limiting their processing in the future. This is a fundamental tenet of the new regulation where you should only collect and use personal data when it is absolutely needed.

Special categories of personal data
Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. There are exceptions in Article 9, but in general it is prohibited to process such data. Since it was not forbidden in the past, you may have inadvertently collected and be using such data.

About SugarCRM

SugarCRM enables businesses to create extraordinary customer relationships with the most empowering, adaptable and affordable customer relationship management (CRM) solution on the market.

Unlike traditional CRM solutions that focus primarily on management and reporting, Sugar empowers the individual, coordinating the actions of customer-facing employees and equipping them with the right information at the right time to transform the customer experience.

Based in Silicon Valley, SugarCRM is backed by Goldman Sachs, Draper Fisher Jurvetson, NEA and Walden International. More than 2 million individuals in over 120 countries rely on SugarCRM.

To learn more visit sugarcrm.com or follow @SugarCRM.

eVolpe is a leading SugarCRM Partner in Poland.

Contact Details

eVolpe Consulting Group
Aleje Solidarności 46
61-696 Poznań
Poland

+48 783 372 094
office@evolpe.com
www.evolpe.com

References and further reading

General information about GDPR:
http://ec.europa.eu/justice/data-protection/reform/index_en.htm

For the complete text in 24 languages
http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679