

GDPR and Your CRM System: Making Sure You're Compliant



EXECUTIVE OVERVIEW



The EU General Data Protection Regulation (GDPR) is the biggest shake up to Data Protection in the UK since the Data Protection Act was passed in 1998.

Every business must be prepared and comply with the new laws or face potentially crippling fines. If you hold any data about any identifiable person then this law applies to you. That includes data about your staff, your customers, your prospects, and your suppliers.

This paper aims to set out what the new laws are and what businesses need to do to make certain they are keeping within the law. It looks at how having a CRM system can help to ensure compliance and what to look out for to check your CRM system is compliant.

If you do not have a CRM system it can be very difficult to comply with the requirements of GDPR as your data could be held in many different places such as spreadsheets on individual staff member's computers, or on their mobile phones.

“GDPR is not only the responsibility of the Chief Information Security Officer or Data Privacy Officer, but of the entire C-suite.”

Daniel Grabski, Executive Security Advisor, Microsoft, source: Microsoft blog

WHAT IS GDPR?

The EU General Data Protection Regulation is an EU Regulation which will become law across the whole of Europe on 25th May 2018. It is a significant change to the way businesses are required to collect, process and secure data about individuals.

It gives individuals many more rights over how their personal data is used, lays down rules regarding data security, and imposes massive fines on companies found to be in breach of these rules.

This is not something you can choose to have, it will be the law. You cannot afford to ignore this regulation as the repercussions of non-compliance are severe. A Level 1 breach could incur a fine of up to €10,000,000 or 2% of global annual turnover, and a Level 2 breach can be a fine of up to €20,000,000 (£17,000,000) or 4% of global annual turnover, whichever is the greater. Fines at that level are potentially business destroying.

And, the Brexit vote makes no difference. The UK will still be a member of the EU on 25th May 2018 and therefore must comply, and the UK Information Commissioner's Office have said they will retain all the rules within this legislation even after the UK has left the European Union.

What are the details and how do they affect me?

The GDPR document runs to well over 200 pages detailing exactly the rights of individuals and the responsibilities of companies. This document can only highlight the most significant areas. To start with we need to explain the key terms used throughout this document.



KEY DEFINITIONS

- **Personal data** – any data referring to a living individual. This includes identifying information such as name, address and email. It also includes any information you may have about someone you met while networking for example: married, two kids, father has dementia. The sort of notes you might make to trigger your memory when you next speak to that person.
- **Sensitive personal data** – this is very specific personal data that would never normally be in the public domain. It includes racial or ethnic origin, political opinions, membership of trade unions, religious beliefs, health conditions both physical and mental, sexual orientation, and criminal offence history. If in doubt, imagine the data is held about yourself – if you wouldn't want the world to know, then it probably counts as sensitive personal data.
- **Consent** – this must be “freely given, specific, informed and an unambiguous indication of the data subject's wishes which may be communicated either by a statement or by clear affirmative action. Consent also has to be a positive indication of agreement to personal data being processed – it cannot be inferred from silence, pre-ticked boxes, or inactivity.” Information Commissioner's Office.
- **Data controller** – the person (or business) who determines the purposes and the way, in which personal data is processed.
- **Data processor** – Anyone who processes personal data on behalf of the data controller (excluding the data controller's own employees). This could be storing the data on 3rd party servers or conducting analysis of the data. Cloud CRM companies are data processors.
- **Data Protection Officer** – The person responsible for data protection within your organisation. If the core activity of the business is processing which requires regular and systematic monitoring of data subjects on a large scale, or, processing of sensitive personal data on a large scale, you will need to appoint a Data Protection Officer. This person can be an employee or an external consultant.
- **Data breach** – when sensitive, protected or confidential data has potentially been viewed, stolen or used by an individual unauthorized to do so. This would include anything from being maliciously hacked to leaving a laptop on the train.
- **ICO** – Information Commissioner's Office – the data authority in the UK.

THE RIGHTS OF AN INDIVIDUAL AFTER GDPR BECOMES LAW:

- The right to be informed. Before collecting and storing any personal data the individual must be informed as to what data will be stored, what it will be used for, and what rights the individual has, to have that data amended or deleted.
- The right of access. Individuals can request details about what personal data is held about them, who has access to it and how long it will be stored. This request must be honoured within one month.
- The right to rectification. An individual can request that any errors in the data be corrected. This must be done within one month.
- The right to erasure. This has been dubbed 'the right to be forgotten' by the press. As it suggests, this is the data subject's right to be completely erased from your database.
- The right to restrict processing. While a data subject may consent to you holding data about them as they are a customer or a client, they have the right to refuse to allow their personal data to be used for example, for marketing purposes.
- The right to data portability. An individual may ask for his or her data in a format they can take elsewhere. This should be provided in a data readable format – the guidelines suggest providing in .csv format.
- The right to object. The data subject can object to how you are using the data, in which case, you must stop using it that way. It must be clear in both your privacy notice and your first communication with the individual how you intend to use the data, and that they have the right to object.

Companies will need to put processes and procedures in place to satisfy these rights. Using a CRM system will make this a much easier task.



'2016/17 saw a 12% increase in public reported incidents to the ICO, up to 18,354 complaints. 64% of which required an action from the nominated data controller.'
(source: ICO)

THE RULES FOR BUSINESSES UNDER GDPR:

“Consent is not the ‘silver bullet’ for GDPR compliance”

Elizabeth Denham, Information Commissioner, ICO, Source: ICO Blog.



1. Businesses must keep a comprehensive record showing how and when consent was given for the data to be used. This consent must be explicit, not inferred.
2. When an individual asks to be forgotten their data must be permanently deleted from a company's business systems, both digital and paper records.
3. Data breaches must be reported to the ICO within 72 hours of the breach together with plans for how the effects of that breach will be dealt with. The individuals whose data has been compromised must also be informed within 72 hours.

WHAT TO DO NOW:

With less than a year to go before GDPR becomes law it is important to start taking action immediately. These are some of the steps you will need to take:

1. Carry out an audit of your data. What personal information do you hold? Where and how is it stored? How is it collected? What processes are in place for obtaining this data? What security is in place to protect the data?
2. Assess your processes and procedures. How can you make your customers and prospects fully aware of how and why information is taken, processed, and stored? And how are you gaining permission to use it?
3. Ensure there are simple processes for individuals to remove consent and, if desired, to be forgotten.
4. Set up a process to answer any data requests.
5. Talk to your technology providers. Is your CRM fit for purpose? What is your CRM supplier doing to ensure compliance? What support are they offering? (See later in this report re: CRM systems).
6. If possible, centralise your data storage to reduce risk.
7. Ensure storage is secure with firewalls, virus monitoring, strong passwords, access control, encryption etc.
8. Develop policies and procedures to ensure compliance with GDPR.
9. Raise awareness within your organisation. Ensure people understand the changes and their responsibilities.
10. Review your privacy policies and statements. These will probably need updating in order to comply.
11. Check if you need to appoint a Data Protection Officer and determine who that will be and what training they might need.

HOW CAN A CRM SYSTEM HELP?

What is a CRM system?

A Customer Relationship Management (CRM) system allows you to manage the business relationships you have with customers, and also colleagues, suppliers and prospects. Organising these relationships helps you market to them more effectively and, hence, grow your business.

The CRM system is a central place to store customer and prospect contact information that can be shared with your colleagues. You can then track every communication with those people including phone calls, emails, meetings, and enquiries.

The CRM system allows you to more fully understand your customers so you are better able to upsell or cross-sell to them.



How can my CRM system help with GDPR compliance?

GDPR requires you to look after data properly, to obtain explicit consent to use it, and to store it securely. And, be able to prove that you have done all that. If you do not have a CRM system it can be very difficult to comply with the requirements of GDPR as your data could be held in many different places such as spreadsheets on individual staff member's computers, or on their mobile phones.

A good CRM system enables you to centralise all your data and control the collection and security of that data. Your CRM system will keep an audit trail of changes to records which will provide proof if and when needed.


Your CRM system should be able to:

1. Record all a contact's consent choices
2. Provide a way for individuals to update or withdraw their own consent online
3. Monitor your organisation's compliance with consent over time
4. Provide a way to respond to data access requests

The CRM system should also be secure with systems in place to prevent, detect and respond to any data breaches.

The major CRM providers such as Microsoft (Dynamics 365), Salesforce, and others are working hard to ensure their software is GDPR compliant before 25th May 2018.

If you are running an older CRM system it may not have the capability to be compliant with GDPR. For your own peace of mind, it is important to check the functionality you have available and what your supplier is doing to ensure the CRM system is compliant.



**“GDPR is an evolution
in data protection, not a
burdensome revolution”**

**Steve Wood, Deputy Commissioner
for Policy, ICO, Source: ICO Blog**

SeeLogic asked its clients what their biggest questions were regarding GDPR. Here are a sample of those questions and our answers.

Q. What is GDPR?

A. Legislation that will come into force on 25th May 2018 affecting the way every business collects, uses and stores personal data. It is not something you have any choice over. It will become law with severe penalties for infringements.

Q. We hold information on individuals' physical conditions as we deal with physically disabled people, including children (minors), and those suffering from dementia.

A. Neither children nor those suffering from dementia can give informed consent. In those cases, consent must be provided by a parent or responsible adult or someone holding a Power of Attorney.

Q. Classifying photos as personal information has always been uncertain. What is the position on this following the GDPR, i.e. if we take photos at an event are they classed as personal information?

A. Whether a photograph counts as personal information depends on how it is processed and used. According to the ICO, police photographing crowds to identify trouble-makers is personal information, a photo journalist photographing the same crowds to record the event is not personal information.

Q. We often hold events and take pictures to use for publicity. Is it correct that the GDPR stipulates we must have explicit permission from data subjects to use pictures from which they can be identified, i.e. we can no longer rely on a notice announcing our intention to take pics?

A. See answer above regarding classifying photos. As now, you need permission to use images of people and you must give them the option to be excluded or blurred out.

Q. It is indicated that we must provide, at the point of gaining consent, all requisite information regarding the processes to which the data will be subject, how can this be done?

A. This will depend on how you are collecting the data. If it's through a sign-up form on your website there should be explanatory text on that page and in your privacy / data usage policy. If you collect information on paper there must be fully explanatory text on the sign-up sheet and a tick box to collect explicit consent.

Q. Following a request from a data subject to be ‘forgotten’, do we have to make every endeavour to remove their information from all requisite backups and archives, and what if this is not possible? Also, what steps should we take if we restore from a backup?

A. You must keep track of requests to be forgotten so that you can re-delete them if you have restored from a backup. It is probably not practical to delete single records from a backup. Any paper records of the person should also be destroyed. You will not have to delete a data subject’s personal information if this information is required for ongoing legal action.

Q. What will be the position if we use a CRM system that has inadequate protection of personal data?

A. A data controller has a specific duty to carry out due diligence on processors before appointing them. If the system is inadequate then you will be liable. Where the data processor is at fault for a data breach it will be treated as a data controller and will be liable.

Q. I have several years of data in my CRM system, do I have to ask all of them for their opt-in to receive future communications from me?

A. If you intend to use the data for marketing purposes you must have consent to contact those people. If you can demonstrate you have consent under the existing Data Protection regulations then you can send an email and ask them to specifically opt-in for further communications under GDPR. If they don’t specifically opt-in then you will have to take that as an opt-out under GDPR. If you cannot demonstrate you have consent under the existing legislation then you will be committing a breach if you send an email asking them to confirm. And should any of the recipients report you to the ICO then you may be fined.

Q. If I have been given a business card at an exhibition or a networking event, can I add that person to my database and start communicating with them?

A. If you wish to communicate with them, you need to request their opt-in in writing. When you meet people at events, ask them if they would be happy to receive communications from you, and if they say yes, inform them that they will receive an email to confirm that, just so you comply with the new GDPR legislation. They must then click on a link in the email, or respond to you, to confirm their consent.

Q. If someone has put a business card in our bowl for a prize draw, can we send them information about our services?

A. No. The information about the prize draw must include the statement that “by placing your business card in the bowl, you are only entering to win the prize draw. This does not constitute your opt-in to receive communications from us going forwards”. It would be worth asking them at the time of putting their card in the bowl, if they are happy to receive communications from you going forwards, when you can inform them that they will receive an email to confirm that as well. See answer above.

Q. I want to target a new list of prospects and I’m planning to buy that list from a list broker. Am I allowed to contact them, as they don’t know me yet?

A. Anyone handling a list will need to make the people on the list aware of specifically how their data is going to be used. E.g. If you are registering for an event and at the end of the form it may currently state “XYZ company sometimes allow their partners access to XYZ’s data, tick here if you are happy to receive communications from those partners.” After GDPR, the information would need to be more specific and detail exactly who those partners are and how they are likely to use the contact details, so one can be more informed and choose to tick the box or not.

Q. Can I charge a fee for responding to a subject access request?

A. The current £10 fee for subject access requests has been abolished. A charge can be made for repeated requests at your discretion.

Q. Do I have to get consent in writing?

A. You have to be able to prove you have consent. Consent in writing will count as proof. An audit trail of someone opting in on a website will also count as proof.

Q. Do we have to pseudonymise¹ ALL personal information and asap? What’s the implications for securing and holding the data access key to allow decrypting?

A. The overarching requirement is that the data is secure. If you are sharing personal data with another company, perhaps for research, then it must be anonymised before sharing and the receiving company must not be able to decrypt that data. As part of data security, if you have pseudonymised your data, the access keys must be kept secure.

1 Pseudonymised data is where the most identifying fields within a database have been replaced with artificial identifiers or pseudonyms. For example, a name is replaced with a unique number.

SUMMARY

GDPR will become law in the UK and across Europe on 25th May 2018. After that point, any company found to be in breach of the regulations could face massive fines. Although it may seem daunting, GDPR is a positive step that will improve consumer trust and marketing activity. The key is to be prepared. Don't wait and hope you'll not be caught, take action now to ensure your data is compliant before the legislation is enacted.

You will need to clean your existing database and set procedures in place to ensure all future data collection complies with the new laws. At the same time review your CRM system to ensure it is compliant and holding your data securely.

And if you don't have a CRM system currently, consider getting one to ease the control of your data going forward.

Disclaimer: The information in this document is for general information purposes only. Nothing in this document should be construed as legal advice. If you need advice on your rights or responsibilities or legal advice, please contact an advisor or solicitor.

METHODOLOGY AND CITATIONS

This White Paper was created using desk research using the following sources:

The Information Commissioners Office at <http://www.ico.org.uk>

Presentation notes from A Tidal Wave on the Horizon: The New General Data Protection Regulation delivered by Matthew Holman of EMW Law llp on 22nd March 2016.

<http://www.b2bmarketing.net/en-gb/resources/blog/gdpr-8-things-you-need-do-right-now>

<http://www.eukhost.com>

<http://touchstonecrm.co.uk/blog/>

<http://www.silicon.co.uk/cloud/google-cloud-gdpr-210937>

<http://www2.cipd.co.uk>

<http://www.itpro.co.uk>

Aylesbury Public Library

ABOUT SEELOGIC

SeeLogic is an independent CRM, ERP and Cloud Technologies specialist, helping businesses drive digital transformation through innovative strategies and solutions. This in turn helps them become more customer-centric, profitable and agile. Our approach is to get to know your business strategy, objectives and goals. We then work with you to review and improve business processes to support the strategy, aligning them with best-fit technologies. SeeLogic will ensure user buy-in through the development of change management strategies – ensuring the impact of the new system is fully realised and effectively managed.

SeeLogic is able to deliver GDPR compliant CRM implementation, as well as offer a range of GDPR consultancy services and solutions. To find out how we can help your business become more customer-centric, profitable and agile, please contact us.

WAYS TO GET IN TOUCH:



01296 328 689



www.seeellogic.co.uk



info@seeellogic.co.uk



[@SeeLogicCRM](#)

SeeLogic



SeeLogic – Your destination for everything CRM,
ERP and Cloud Technologies based