What is GDPR?

The General Data Protection Regulation (GDPR) comes into effect on 25th May 2018. In the UK it will replace the Data Protection Act 1998 (DPA). The GDPR will ensure that all companies that use personal information of European residents only do so in accordance with the privacy and other standards set out in the GDPR.

In some cases, there has been just a slight change or enhancement to the concepts and principles of DPA. For example:

- What makes up personal information
- Protecting medical and other very personal information
- Subject Access Requests

In other cases, GDPR introduces new regulations and requirements such as:

- Stronger personal rights
- Being able to stop automated processing
- Stronger accountability principles

Organisations which openly communicate how they work within GDPR are likely to be trusted by prospects and customers, so offer a serious competitive advantage over competitors. Conversely, failure to comply with GDPR can lead to monetary fines and loss of reputation.

Territorial Scope

All the rules, policies, restrictions and user rights defined by GDPR are applicable to companies that deal with personal data of EU citizens. This will also include organisations based within and outside the EU.

Defining Personal Data

GDPR defines personal data as "any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier". This is wider than the terms defined by the DPA. In addition to the existing identifiers, it also takes into account data such as:

- IP addresses
- Mobile device IDs
- Behavioural data
- Financial information (in some circumstances)

Much of the information about individuals (as opposed to companies and similar organisations) that we record in the CRM system is likely to be considered as "personal data" under GDPR. It is thus of paramount importance that we ensure security in:

- Data creation
- Data storage
- Data management
- Data use

Accountability Requirement

As a highly flexible and customisable solution ACT offers a wide variety of features that can help users to manage their data processes, privacy and security effectively.

It can be an extremely valuable tool to help with GDPR when used and adopted within your business, as part of a wider GDPR compliance project.

CRM Systems have a number of features that can help you record majority of actions that take place on personal user data:

Tracking the source of data record within a field.

Adding supplementary attachments against a record such as:

- Email correspondence
- Scanned Documents
- Call Recordings

Time stamped notes and history data can be added against an individual contact.

Configure fields to automatically add history entries when their contents are changes ensuring traceability of made changes.

Data Usage

Like the DPA, the GDPR contains data protection principles which set out the principles organisations must follow when processing an individual's data.

Data must be:

- Used fairly, lawfully and transparently.
- Collected for specified purposes, and then used in a way that is in accordance with those purposes.
- Kept Securely
- Only kept for as long as it is necessary for the in the initially specified purposes. Depending on your business requirements, you should formulate a policy that signifies how you distinguish between obsolete and useful data and define processes for identifying and managing the former

CRM Help with these requirements

These first requirements are all closely related. CRM can help you to:

- Keep track of how data is being created, changed and used with reports on record information.
- Limit access for specific employees to specific data depending on their roles.
- Store customer preferences regarding data usage in the database which can be displayed to any used by employees during communications, e.g. if a customer doesn't want to receive a weekly newsletter.
- Field level security can be used to ensure that users are able to only view or change data that is pertinent to their role.
- A password policy can be defined in most CRM systems, enabling you to govern the length, complexity, change frequency and reuse of prior passwords.
- Automatically recording the created date and last edit date of each record, which can be eventually be used as query parameters to determine record age and ongoing relevance.
- Creating groups or filters to automatically segment and highlight records matching your filtering criterion.
- Providing search functionality which allows you to perform complex records on data collection criteria.
- Allow users to manually flag records for deletion or create automation to do that function.

Lawful basis for processing

Organisations need a lawful basis to process data. This was a very similar under the DPA, though accountability for and transparency about any basis is now more important.

There are six lawful bases for processing:

1. Consent: Individuals must give this clearly and in relation to a specific process.
2. Contract: Processing is necessary for a contract or to enter into one.
3. Legitimate Interests: The processing is necessary for your interests, or some other parties unless there is a good reason to protect the individual's personal data which is more important than those interests.
4. Legal obligation: Not including contractual ones.
5. Vital Interest: To save someone's life.
6. Public Task: This will only apply to public sector organisations.

Consent

Consent is often used as a lawful basis.
It must be freely given, specific, informed and unambiguous indication of the individual wishes.

There must be some form of clear affirmative action – or in other words, a positive opt in. Consent cannot be inferred from silence, pre-ticketed boxes or inactivity.

Consent must also be separate from other terms and conditions, and you will need to provide simple ways for people to withdraw consent.

Consent must be verifiable, and you need to build in methods for individuals to exercise their rights about giving consent. The information commissioner's Office (ICO) website says, "you are not required to automatically refresh all existing DPA constants in preparation for the GDPR. But if you rely on individuals' consent to process their data, make sure it will meet the GDPR standard on being specific, granular, clear, prominent, opted-in, properly documented and easily withdrawn. If not, alter your consent mechanisms and seek fresh GDPR-compliant consent, or find an alternative to consent."

CRM Help with these requirements

CRM systems can usually help with managing opt-ins. E-marketing for example has an unsubscribe option and custom fields can be created in the database to provide granular opt in options.

Search or filters and lists can also be used to manage lists of contacts who have opted out of mailings or don't want to be communicated to.

Individual Rights

GDPR expands on the rights an individual has over how their personal data can be used.

The right to be informed

GDPR requires companies to inform individuals when collecting their data. The extend of the information you supply is determined by whether or not you obtained the personal data directly from individuals (more information on the ICO's website).

Most of the information you should supply is consistent with your current obligations under the DPA, but there is some more information that you have to explicitly provide. The information about the processing of personal data must be:

- Concise, transparent, intelligible and easily accessible.
- Written in clear and plain language, particularly if addressed to a child
- And free of charge.

CRM Help with these requirements

Through customisation, a field can usually be created in CRM systems to record the appropriate information has been given and when.

A drop down could be used within a field to specify the source via which the permission was given for example via a phone call, web contact form etc.

The right of access

The GDPR right of access is similar to its DPA counterpart, but information must now be provided free of charge, unless the request is “manifestly unfounded or excessive” when a reasonable fee can be charged.

In summary information must be provided without delay and within **one month** of receipt. There is an obligation to verify the identity of the individual making the request using “reasonable means”.

Requests made electronically should be responded to in a commonly used format. There is a best practice recommendation that, “where possible, organisations should be able to provide remote access to a secure self-service system which would provide the individual with direct access to his or her information. This will not be appropriate to all organisations, but there are some sectors where this may work well

CRM Help with these requirements

CRM systems will easily provide various reports including a detailed contact report which can be generated against an individual, providing a full account of the information stored about them.

Most CRM systems will also enable data held within the contact fields to be exported to a number of file formats including .csv for easy sharing with the subject.