GDPR Compliance

How CRM systems can help businesses to comply with the General Data Protection Regulations

What is the GDPR?

The General Data Protection Regulations (GDPR) come into effect on 25th May 2018. In the UK they replace the Data Protection Act (DPA) of 1998. 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.

Some of the regulatory concepts and principles of DPA – for example what makes up personal information, protecting medical and other very personal information, subject access requests - have only slightly been changed or enhanced by the GDPR. However GDPR introduces new regulations and requirements – for example stronger personal rights, like being able to stop automated processing, and stronger accountability principles.

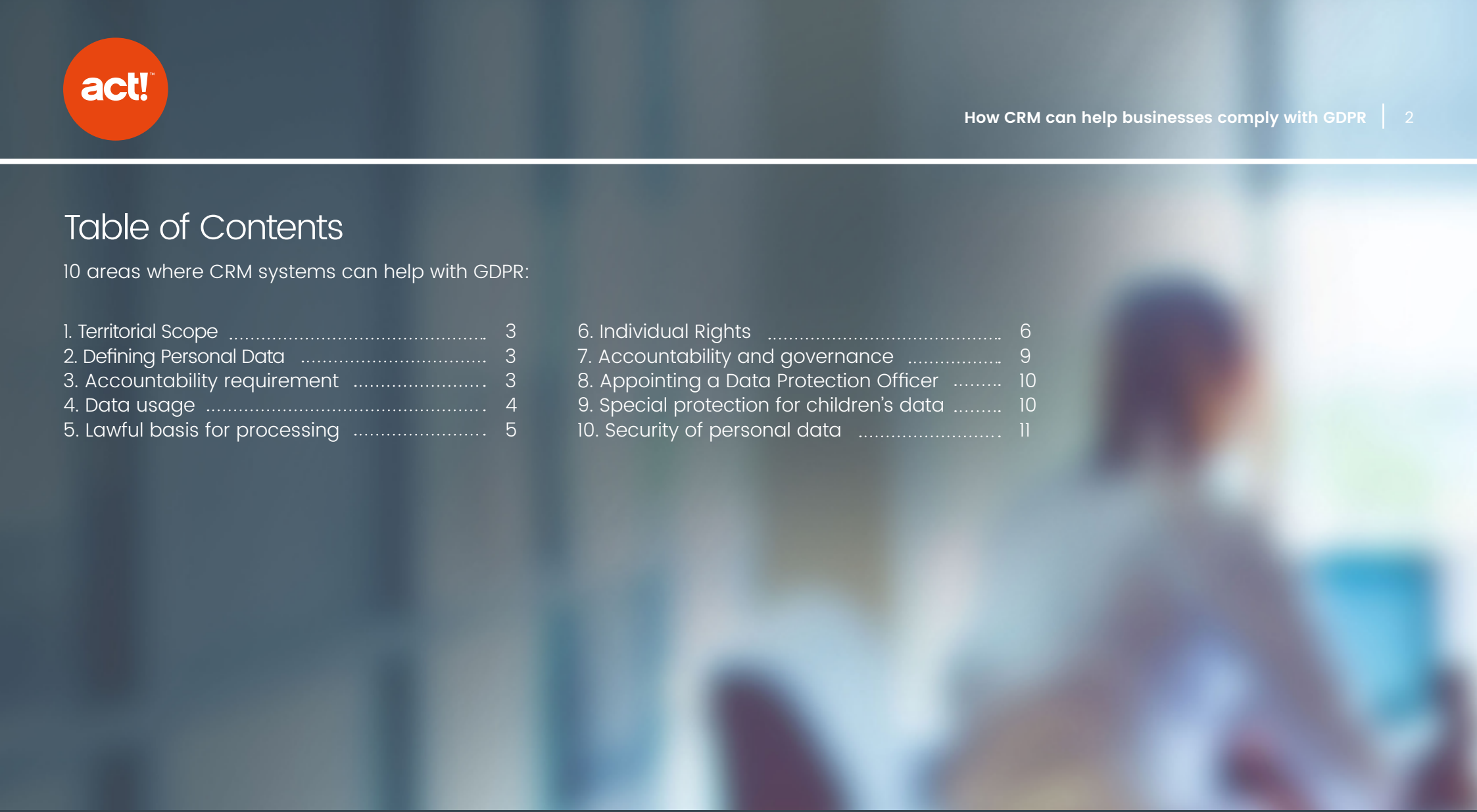
GDPR and CRM systems

Organisations which communicate openly how they work within GDPR are likely to be trusted by prospects and customers, so have a serious competitive advantage over competitors. Conversely, failure to comply with GDPR can lead to monetary fines and loss of reputation. So it is important that companies have an ongoing approach to reviewing and updating their business processes and policies, to become and remain GDPR compliant.

Most CRM systems are highly flexible and functional relationship management systems, offering a wide variety of features that can help users to effectively manage their data processes, privacy and security. If you are already using a CRM system - or considering it - you will likely be aware that it can be an extremely valuable tool to help with GDPR compliance if correctly adopted and used within your business. This document has been written to help you understand some key GDPR concepts, and to provide information about how using a CRM system can help with becoming compliant.

Table of Contents

10 areas where CRM systems can help with GDPR:



Disclaimer: The information contained in this guide is not legal advice, and does not cover all of the ways in which GDPR can impact your business. We recommend working with a legal specialist to help you fully assess your business requirements for GDPR, and ensure compliance.

1. 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 includes organisations established within and outside the EU. So even if your company is based in the US and you have records about individuals resident in the EU, you will have to process their information in line with GDPR.

With most CRM systems you have the ability to record a user's residential country, which then makes it straightforward to identify and report on individuals that have rights under GDPR. You can also group all the relevant records for easy management.

2. Defining Personal Data

The 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 term was defined in the DPA. In addition to the established identifiers, it also takes into account data such as IP addresses, mobile device IDs, behavioural data and, in certain circumstances, financial information.

Much of the information about individuals (as opposed to companies and similar organisations) that you record in the CRM system is likely to be considered "personal data" under GDPR. Hence, it's of paramount importance that you ensure that data creation, storing, management and use is done in a compliant manner. It's not only important to keep the data secure, but you also have to make sure that it's only kept for as long as it is needed.

3. Accountability requirement

The GDPR requires you to document and maintain records on how you use and store (or 'process') personal information. For SMEs, documentation is only necessary for certain processing.

Most CRM systems have a number of features that allow you to record majority of the actions taken place on personal user data:

- Tracking the source of a data record within a field.
- Adding supplementary attachments against a record, such as email correspondence, scanned documents, call recordings etc.
- Time stamped notes and history data can be added against an individual contact. This can be used to record an interaction with them, or to document an internal process that was followed.
- Configuring fields to automatically add history entries when their contents are changed; ensuring traceability of any made changes.

4. Data usage

Like the DPA, the GDPR contain 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.

These first requirements are very closely related. Whilst CRM systems can't fully control or limit how you use personal data, it can certainly help you to:

1. Keep track of how data is being created, changed and used using record information. Limit access for specific employees to specific data depending on their roles.
2. Store customer preferences regarding data usage in the database which can be displayed to and used by employees during communication. For example, if a customer doesn't want to receive weekly newsletters and/or product launch emails, the system can classify them as opt-outs.
3. Field level security can be used to ensure that users are able to only view or change data that is pertinent to their role.
4. A password policy can be defined in most CRM systems, enabling you to govern the length, complexity, change frequency and reuse of prior passwords.

- Only kept for as long as it is necessary for 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 defines processes for identifying and managing the former.

CRM systems may help you implement this in a number of ways:

1. Automatically recording the created date and last edit date of each record, which can eventually be used as query parameters to determine record age and ongoing relevance.
2. Creating groups to automatically segment and highlight records matching your filtering criterion.
3. Providing lookup functionality which allows you to perform complex record searches based on when different areas of the record were last changed.
4. Allowing users to manually flag specific records for obsoleteness (deletion) or archiving using a custom field.

5. Lawful basis for processing

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

These are:

Consent
Individuals must give this clearly and in relation to a specific process.

Contract
Processing is necessary for a contract or to enter into one.

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.

Legal obligations
Not including contractual ones.

Vital interests
To save someone's life.

Public task
This will only apply to public sector organisations.

Consent is often used as a lawful basis. It must be a freely given, specific, informed and unambiguous indication of the individual's 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-ticked 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 has to 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 consents 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 systems can usually help you manage opt ins. Act! emarketing for example has an unsubscribe option and custom fields can be created in the Act! database to provide granular opt in options. Look ups and lists can also be used to manage lists of contacts who have opted out of mailings.

To get more information about lawful processing and consent, you can visit the relevant page of the **official ICO website**.

6. Individual Rights

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

6.1 The right to be informed

GDPR requires companies to inform individuals when collecting their data. The extent of 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.

Through customisation, a field can usually be created in CRM systems to record that appropriate information has been given to the individual. For example, a Date Box or a Yes/No field (check/tick box) could be created to note that appropriate information has been given, and when. A drop down could specify the source via which the permission was given (e.g. via a phone call, web contact form etc.)

6.2 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 (Recital 63). This will not be appropriate for all organisations, but there are some sectors where this may work well."

CRM systems will often 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 contact fields to be exported to a number of file formats (including .csv) for easy sharing with a data subject.

6.3 The right to rectification

Individuals are entitled to have their data rectified if it is inaccurate or incomplete. This must be done within a month, unless the request is complex, in which case there is a possibility for an extension. If no action is being taken, that must be explained to the individual, along with their rights to complain. Third parties to which data has been relayed to will also be required to rectify the data.

CRM systems will likely enable a record to be made of the rectify request, using a note, or the "history", when the "created date" will usually be stored. Follow ups to the request could be recorded as an additional history entry or activity against a specified user.

A CRM system could be used to record if and when information gets shared with a third-party; this can facilitate contacting them in case a rectify/erasure request is made.

A process should be put in setting out the steps an employee must take when they receive a request for rectification.

6.4 The right to erasure

Also known as the right to be forgotten, the right to erasure enables an individual to request the deletion or removal of personal data if and when there is no compelling reason for its continued processing. Individuals have a right to have personal data erased and to prevent processing in specific circumstances. Third parties to which data have been passed must also adhere to the guidelines.

CRM systems usually allow the deletion of contact records, which will in turn delete all entries and data associated with the record (unless these are associated with other contacts). The deletion should usually be recorded in the section which records the actions of all users of the system – for example who performed the deletion, noting the date, time, and contact name.

In this way the CRM system can be used to record where information has been shared with a third-party to facilitate contacting them should this be erased.

6.5 The right to restrict processing

Like in the DPA, individuals have a right to block processing of personal data. When processing is blocked, an organisation is permitted to continue storing the personal data, but any further processing is prohibited.

A custom field can be used to track any customer's instruction to restrict processing.

6.6 The right to data portability

Individuals may obtain and reuse their personal data for their own purposes across different services. They should be able to move, copy or transfer data from one IT service to another, securely and without any hindrance. The processor has to respond within a month of receiving such a request. The personal data must be provided in an open format that is structured, commonly used and machine-readable. You may have to transmit the data to another organisation if that is technically feasible. You shouldn't prejudice the rights of others, e.g. by disclosing third party data.

Again, it will usually be relatively easy to export data held within contact fields to a number of file formats (including .csv).

6.7 The right to object

If a processor processes personal data for the performance of a legal task or for the organisation's own personal interests, an individual can object based on 'grounds relating to his or her particular situation'. The organisation must stop, unless there are substantially legitimate grounds for the processing which override the rights of the individual, or if the processing is for exercising legal claims.

Individuals must be informed of their right to object at the point of first communication and in the privacy notice. This notice must be explicitly brought to the attention of the person and be presented clearly and separately from any other information. If the processing activities are carried out online, there must be a way for individuals to object online. As this is an important area we suggest you to read the Information Commissioner's guidance in full, click here to do so.

Your CRM system should allow email recipients the ability to opt out of any future campaign emails, in the footer of the email they receive as part of your campaign. For example, if you are using Act! emarketing you can track recipients who have opted out of your campaigns.

6.8 Rights in relation to automated decision making and profiling

The GDPR gives individuals rights when they are the subject of automated decision making and profiling. (The ICO describes profiling as "automated processing of personal data to evaluate certain things about an individual".) These rights are stronger when automated decision making and profiling has a legal or similarly significant effect on an individual. As this is a relatively complex area and can involve considerably sophisticated technology, please read the detailed information available on the ICO website, here.

With Act!, users can manage automated decision making with a feature called 'Smart Tasks'. Users of this feature should ensure that the steps of 'Smart Tasks' are reviewed regularly to avoid a potential breach of GDPR. An example of this would be setting up a 'Smart Task' to run when certain conditions are met; a customer who has opted out of your emails could be sent an automated email if the information within their contact record is not up to date.

CRM administrators should ensure that their business and legal advisers understand that it is possible for automated decision making and profiling to be carried out through its use and hence appropriate disclaimers should be included in privacy notices. Relevant processes should be considered, for example to stop making automated decision making and profiling of an individual in the required circumstances. This enables users to provide customers with their data which is being used for automated decision making and profiling, and to flag contacts who fall into the 'vulnerable group' category under GDPR.

7. Accountability and governance

The GDPR requires that organisations put into place comprehensive but proportionate governance measures. The ICO says that to demonstrate compliance an organisation must:

• "Implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies;

• maintain relevant documentation on processing activities;

• where appropriate, appoint a data protection officer;

• use data protection impact assessments where appropriate;

• implement measures that meet the principles of data protection by design and data protection by default. Measures could include:

- data minimisation;
- pseudonymisation;
- transparency;
- allowing individuals to monitor processing; and
- creating and improving security features on an ongoing basis.

You can also adhere to approved codes of conduct and/or certification schemes."

Use of a CRM system like Act! is incidental to much of the scope of this part of the GDPR. Importantly, each organisation must implement compliance processes, for example documenting compliance and carrying out Impact Assessments. They should also adopt relevant procedures to meet requirements set by the principles of data protection by design and default. Organisations should consult the ICO's website for more information and work with consultants to ensure they put in place and maintain the appropriate governance measures.

Data protection by design and default

There is a general obligation on processors to implement technical and organisational measures to show they have considered and integrated data protection into their data processing activities and processes.

Privacy by design "is an approach to projects that promotes privacy and data protection compliance from the start... The ICO encourages organisations to ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle. For example when:

• building new IT systems for storing or accessing personal data;

• developing legislation, policy or strategies that have privacy implications;

• embarking on a data sharing initiative; or

• using data for new purposes."

A Data Protection Impact Assessment should be carried out when considering the use of new technology. The Information Commissioner has a Code of Practice explaining how to use Impact Assessments. Carrying out one should "reduce the risks of harm to individuals through the misuse of their personal information. It can also help you to design more efficient and effective processes for handling personal data".

In this scenario, a CRM is most likely to be useful as a document repository. For example, in Act! Premium Plus, if "Projects" have been created as an entity using the Custom Tables Manager, the written Impact Assessment on each project can be stored along with other documentation; for example any business case or project initiation document.

Codes of conduct and certification schemes

It should be noted that the pertinent codes of conduct and certifications need to be endorsed by the UK ICO (if an organisation has determined the ICO is their relevant supervisory authority). At the time of writing (April 2018) we are not aware of any code of conduct which has been approved by the ICO or certification which has been certified by it, that would be relevant to the use of Act! CRM.

For more details, the relevant section of the ICO's site is here.

8. Appointing a Data Protection Officer

This is required in certain circumstances only. Regardless of whether an organisation is obliged to appoint one, it must have sufficient skills and resources to comply with the data protection requirements. The DPO's minimum required tasks are defined here.

9. Special protection for children's data

If your company offers its products or services to children then you might need to get the consent of their parents or guardians before collecting or processing any of their data. Under GDPR, only a person aged 13 or over can give their own consent. More information about this can be obtained from the relevant page of the ICO website.

With a CRM system you can store the age against every new contact and then perform a lookup to identify children for whom you have a record. You can then take appropriate steps to process those children's information in line with GDPR requirements.

10. Security of personal data

Personal data must be processed securely by taking appropriate technical and organisational measures. You should do a proportionate risk analysis and put in place relevant organisational policies and take appropriate technical and physical measures. Anonymisation and encryption should be considered. Systems and services must keep personal data confidential and secure and maintain its integrity. Back ups should be made to enable lost data to be restored. Whatever measures are put in place should be tested and any necessary improvements made. More information is available on the ICO's website at this link.

Transfer of data outside the EU

Personal data can only be transferred when specified conditions are met.

There are a number of schemes that have been put in place by regulatory bodies, following decisions of the European Commission.

There are exceptions to the general prohibition for certain specific circumstances – when the transfer is:

- made with the individual's informed consent;
- Necessary for the performance of a contract between the individual and the organisation or for pre-contractual steps taken at the individual's request;
- Necessary for the performance of a contract, made in the interests of the individual, between the controller and another person;
- Necessary for important reasons of public interest;
- Necessary for the establishment, exercise or defence of legal claims;
- Necessary to protect the vital interests of the data subject or other persons, where the data subject is physically or legally incapable of giving consent; or
- made from a register which under UK or EU law is intended to provide information to the public (and which is open to consultation by either the public in general or those able to show a legitimate interest in inspecting the register).

In certain limited circumstances, one-off transfers of data of relatively few individuals are permitted.

Breach notification

Data processing organisations have an obligation to notify of breaches if they are likely to result in a risk to the rights and freedoms of individuals – a breach which if nothing is done will have a significant detrimental impact on individuals. For example, if it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or other significant economic or social disadvantage. Individuals must also be notified when the involved risk is high.

Notification must be issued to supervising authorities within 72 hours, and if necessary, to individuals without undue delay. Failing to do so can result in a significant fine (up to €10M or 2% global turnover).

It's important for a company to take steps regarding staff education, internal breach identification, investigation and reporting procedures.

Join over six million users in 170 countries to create your adaptable, everywhere, and connected workspace today.

What is Act!

Act! makes it easy to build relationships that last with quick, organised access to highly personalised customer details. Because every business runs differently, you have the freedom to tailor an Act! experience to your business and industry needs—your adaptable, everywhere, connected workspace. Finally, a CRM solution that's unique to you.

Call 0845 268 0220
visit act.com/uk
or contact your Act! Certified Consultant[1]

1 Act! Certified Consultants are third-party vendors. Swiftpage and its affiliates are in no way liable or responsible for claims made related to the services provided by third-party vendors.

Q15, Quorum Business Park, Benton Ln. | Newcastle Upon Tyne, NE12 8BU | 0845 268 0220 | act.com/uk