GDPR Compliance

How Act! CRM can help businesses comply with
the General Data Protection Regulation

What is the GDPR?

The GDPR applies to the use and storage of personal information of European citizens from 25 May 2018. All organisations world-wide need to comply with them if they want to comply with European law. The GDPR has an organisation-wide impact and this document explains how Act! can help an organisation to comply.

The General Data Protection Regulation (GDPR) comes into effect on 25th May 2018. In the UK they replace the Data Protection Act (DPA) 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 Act! CRM

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

As a highly flexible and customisable solution, Act! CRM 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 compliance if correctly used and adopted within your business, as part of a wider GDPR compliance project. This document should help you understand some of the key areas of GDPR, and provide information about how using Act! CRM can help with compliance.

Table of Contents

9 areas where Act! CRM can help with GDPR:

1. Defining personal data 3
2. Controllers and processors 3
3. Territorial scope 3
4. Data protection principles 4
5. Lawful basis for processing 6
6. Individual rights 7
7. Accountability and governance 13
8. Appointing a Data Protection Officer 15
9. Security of personal data 15

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. References to features relate to Act! Premium and Premium Plus version 20.1.

1. Defining personal data

Personal data is any data which can be used by itself, or combined with other data to identify an individual. Under GDPR, the term 'personal data' is defined more widely than it was under the DPA – and takes into account a wide range of things that could identify a person such as unique identification names/numbers, IP addresses, online behavioural data and location data.

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 is only kept for as long as it is needed.

2. Controllers and processors

An organisation which determines how and for what purposes personal data is processed is called a 'controller'. A processor processes personal data on behalf of a controller. The GDPR place legal obligations on controllers. Processors also have obligations, for example to keep records of processing that has taken place.

3. Territorial scope

The GDPR applies to all organisations established in the EU, as well as organisations processing personal data of EU citizens, even if the organisation is outside the EU.

By recording an individual's country of residence in Act!, you can quickly identify records which have rights under the GDPR. A grouping of these records can also be created for quick and easy reference.

How to create and manage Groups in Act!: Article ID 12864

4. Data protection principles

Similar to the Data Protection Act which GDPR supersedes, there are 6 data protection principles which govern how an individual's data can be used. Personal data must be:

- Used fairly, lawfully and transparently.
- Collected for specified purposes, and then used in a way that is compatible with those purposes.
- Used in a way that is adequate, relevant and the use limited to what is necessary for the specified purposes.

These first requirements are very closely related. Act! can't fully control or limit how you use personal data, but it can help you to:

1 Keep track of how users are creating, changing and using record information.

How to use the History List in Act!: Article ID 36109

2 Limit access for specific users to the records or specific fields that are relevant to their role.

Security Roles in Act!: Article ID 15284

3 Store and clearly display preferences made by individuals stored in the database around how their data is used, so that users can work with the data in respect of this. Opt-ins or opt-outs from specific communications, or interests so communications can be kept relevant. In this example recipients have the option to opt-out of campaigns sent to them via emarketing[1], you can view a list of opt-outs by following the steps in the article below:

How do I create a lookup of my Act! emarketing bounces or opt outs in Act! v17.2 and later?: Article ID 38139

- Only kept for as long as is necessary for the specified purposes.

Your business must determine its own policy for what constitutes obsolete or redundant data, as well as defining processes around for identifying and managing these records. Act! can help you put this in to practice in a number of ways:

1 Automatically recording the Create Date and Last Edit Date of each record, which can easily be searched or filtered on to determine record age and ongoing relevance.

2 Create groups to automatically segment and highlight records matching your determined criteria.

3 Providing Lookup functionality which allows complex record searches based on when different areas of the record were last changed.

4 Allowing users to manually flag specific records for deletion or archiving using a custom field.

The following article allows you to search records for specific field values within Act!:

How to perform a lookup in Act!: Article ID 26841

As well as searching individual fields you can also create a Lookup using AND/OR functions:

How to create an Advanced Query in Act!: Article ID 26794

As well as searching individual fields you are able to setup Groups. You can control which Contacts are members of a Group through Static and Dynamic:

How to create and manage database fields in Act!: Article ID 15335

• Kept in a form which permits identification of data subjects, only for so long as is necessary.

Create Dates and Edit Dates of records can prove when the last interactions have been. These can be used to generate Reports or Look Ups which can then be used to review whether it is still necessary to keep the record. For example users can make decisions based on the dates on which there was last an interaction with, or change to, a Contact.

You can track field changes by enabling History Tracking for specific fields within your database through the Define Fields area of Act! allowing you to record all changes made by any user to individuals' data:

How to create and manage database fields in Act!: Article ID 15335

• Processed in a way that ensures the personal data is kept secure, including protection against unauthorised and unlawful processing, and against accidental loss, destruction or damage. Appropriate technical and organisational measures must be used.

Act! provides a wide range of features governing security and record access. The features allow you to limit access Users have to the data by adjusting their Security Level, or by applying specific permissions to a field. Users' access can be limited meaning s/he will only have access to the data that is pertinent to them, thus reducing the risk of "unauthorised disclosure of, or access to personal data."

Security Roles in Act!: Article ID 15284

Note: In order to set multiple Notes, History, Opportunity entries, or Contacts to Public/Private you require an Offline Client. More information on creating an Offline Client can be found in the following article: How do I set up my Act! Premium Cloud offline client?: Article ID 37973

Act! provides a wide range of functions allowing the management of record and data access:

1. Field level security can be used to ensure that users are able to only view or change the field data which is pertinent to their role.

How to Manage Field Level Security in Act!: Article ID 19185

2. Record access can be stipulated for Contact, Company, Group and Opportunity records, whereby the entire record contents are only visible to the specified user(s) or configured Team of users.

3. Record entries such as notes, histories and activities can be set as Private, meaning they are only visible to the specified record manager.

4. Five default user security roles offer a range of permissions to database functions, ranging from browse only, to full administration. These roles control permissions such as exporting data, and creating, deleting or editing records.

Information on controlling User access can be found on our knowledgebase in the following articles:

How to Change the Public/Private Status of Multiple Notes, History, or Opportunity Entries: Article ID 19189

Review Act! user roles, and ensure the correct security roles and record access is in place for users based on the requirement of their individual roles.

How do I set Contact Access controls for users in Act!?: Article ID 15228

The database synchronisation feature, which allows a remote database to be created, can be based on a 'sync set', where only contact records matching the specified criteria are transferred to the remote user.

How to Manage Remote Database Sync Sets in Act!: Article ID: 14072

In order to amend a 'sync set' in a Cloud version of Act!, you should submit a ticket to our Cloud team here.

A username and password can be set for each individual Act! user. Additionally, a detailed password policy can be configured in Act!, governing the password length, complexity, change frequency and reuse of prior passwords.

You can manage a User through the Manage Users area of Act!; within here you can also set a password:

How to create and manage database Users in Act!: Article ID: 19474

How do I add or remove users to my Act! Premium Cloud database?: Article ID 37948

How to Manage Password Complexity Settings: Article ID 19180

Act! allows backup of data to prevent accidental loss, destruction or damage. This includes a Scheduler feature to automate backups on a specified frequency. These features should be used in conjunction with a robust backup policy.

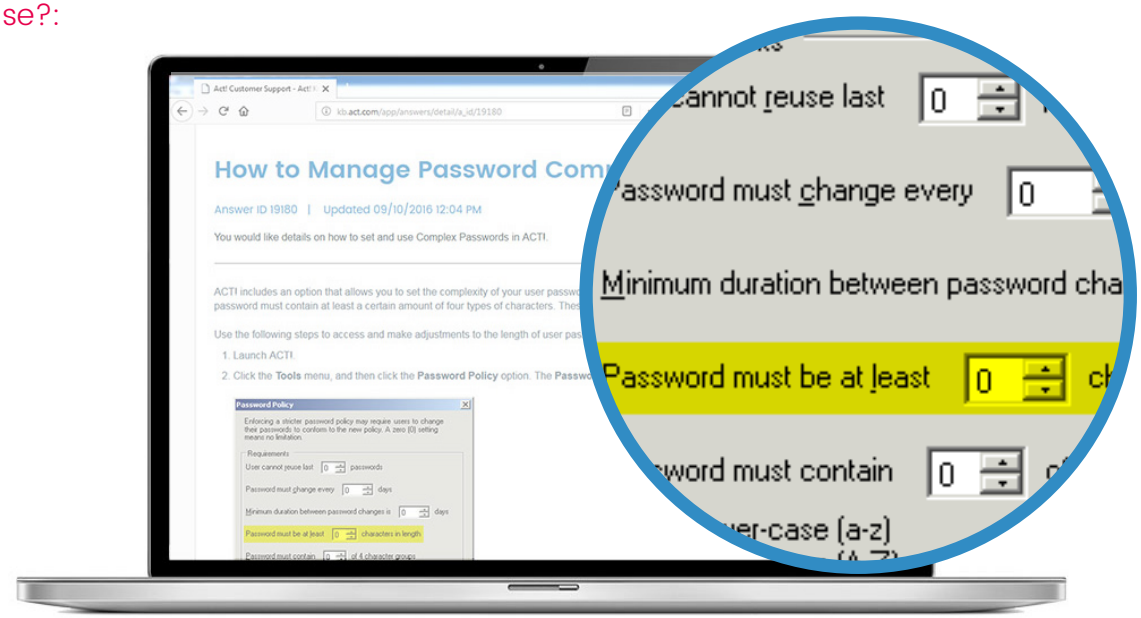
How to back up and restore an Act! database: Article ID 19211

How to use the Act! Scheduler to automatically back up your Act! database: Article ID 19218

If you are using a Cloud version of Act!, Act! backs up databases automatically every 6 hours. More information on backups can be found in the articles below:

How often do you backup my Act! Premium Cloud Database?: Article ID 39080

How do I request to have a backup of my Act! Premium Cloud database restored?: Article ID 39079



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 using, any basis is now more important. There are six lawful bases for processing. In this document we only cover the lawful basis of consent. However, at least one of the other bases are likely to be as relevant a basis for processing, if not more so, as consent. The content on this page of the Information Commissioner's Office (ICO) website is very helpful to determine the bases on which an organisation can rely.

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.
Legal obligations	Need to process the personal data to comply with law.
Vital interests	To save someone's life.
Public task	This will only apply to public sector organisations.
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.

Consent

Consent is often used as a lawful basis in relation to processing for marketing purposes. 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. "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."

The section below will assist in managing consent given via emarketing[1] opt out and opt in.

There is more information available on Consent as a lawful basis for processing in the following article from the ICO website:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

---

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

Similar information as under the DPA needs to be provided when collecting individuals' data with additions. The information you supply is determined by whether or not you obtained the personal data directly from individuals and is set out in a detailed table on the ICOs web pages. Much of the information you should supply is consistent with your current obligations under the DPA, but there is some further information you are explicitly required to provide. The information you supply 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.

Whatever data you gather, individuals need to be kept updated. They need to know what personal information you're storing and what you're going to do with it. All communication with your clients on this subject must be straightforward and free of charge to access.

Through customisation a field can be created in Act! to record that appropriate information has been given to the individual whose details are recorded in a Contact record. For example a Date Box or 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 of permission given (e.g. on phone call, web contact form etc)

How to create and manage database fields in Act!: Article ID 15335

When you have created a field you will receive a prompt asking if you would like to add the field to your layout, there is further information on using the Layout Designer in the article below:

Designing Layouts in Act!: Article ID: 15332

If a customer has a web site then an Act! Web Form could added which provides a 'double opt in' process to the individual filling in the form prior to storing that individual's record as a Contact in Act!. The fact that this has been submitted by the individual can be reported on through Act! emarketing' for auditing purposes.

How to use the Web forms feature (formerly known as Lead Capture) in Act!: Article ID 37906

Users of Act! should consider implementing a process which governs the provision of information to individuals who fill in forms, and recording when and how that information was given.

6.2 The right of access

This is similar to the position under the DPA, 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 in electronic format should be provided 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."

Act! provides a detailed Contact Report which can be run against an individual Contact to provide a full account of the information stored about them.

How to run and manage reports in Act!: Article ID 14022

Data held within Contact fields can also be exported to a number of file formats (including .csv) for easy sharing with a customer.

How to Export Your Contact, Company, or Group Data from Act! to a Text or Comma Delimited File: Article ID 13882

6.3 The right to rectification

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

Act! enables a record to be made of the request to rectify, for example as a History. The create date of the History will be stored. Follow ups to the request can be recorded as an additional History or Activity for a specified User.

Act! can be used to record where information has been shared with a third-party to facilitate contacting them should this be erased.

A process should be put in setting out the steps an employee must take when s/he receives a request for rectification.

6.4 The right to erasure

Also known as the right to be forgotten. This right is to enable an individual to request the deletion or removal of personal data where 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 given in the GDPR. Third parties to which data has been passed must also be informed.

Act! allows the deletion of Contact records, which will in turn delete all entries and data associated with the record (unless these are associated with other, remaining contacts). The deletion is recorded in History of the Act! user who performed the deletion, noting the date, time, and contact name.

Act! can be used to record where information has been shared with a third-party to facilitate contacting them should this be erased.

A process should be put in place around any information passed to third-parties.

How to manually create Histories in Act!: Article ID 38835

6.5 The right to restrict processing

Like with the DPA, individuals have a right to block processing of personal data. When processing is restricted, you are permitted to store the personal data, but not further process it. You can retain just enough information about the individual to ensure that the restriction is respected in future.

A custom field can be used to track the customer's preference on no processing. This would need to be manually adhered to by users of Act!.

How to create and manage database fields in Act!: Article ID 15335

As an additional precaution, contact details such as telephone numbers and email addresses can be moved out of the default fields to prevent accidental contact or inclusion in an email campaign for example. You may wish to move the data to other custom fields that will not be read by Act! to prevent accidental inclusion.

How do I use the Replace, Swap, and Copy options in Act!?: Article ID 38137

6.6 The right to data portability

Individuals may obtain and reuse their personal data for their own purposes across different services. The processor has to respond within a month. They should be able to move copy or transfer data from one IT service to another, securely and without hindrance. 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.

6.7 The right to object

From the perspective of using Act!, the relevant rights based on which individuals may object are:

- Processing based on legitimate interests (including profiling)
- Direct marketing (including profiling).

If a processor processes personal data for the performance of a legal task or 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 is compelling legitimate grounds for the processing which override the rights of the individual, or 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. As now, this notice must be brought explicitly to the attention of the data subject 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 read the ICO guidance in full, see this link: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/

Within Act! emarketing[1], recipients have the ability to opt-out in the footer of the email they receive as part of your campaign. The impact of this is explained in this article.

If a customer opts out from my emarketing campaigns, does the system prevent me from sending to them or do I have to remove the contact's email from my database?: Article ID: 38681

If you are using Act! emarketing[1] you can track recipients who have opted-out of your campaigns by following the steps in the article below:

How do I create a lookup of my Act! emarketing bounces or opt outs in Act! v17.2 and later?: Article ID 38139

If you are using Act! emarketing[1] you can view your opt-outs by following the steps in the article below:

How to access your Act! emarketing opt-out list: Article ID 28591

Can recipients opt back in to my campaigns?

Should your recipient opt-out in error, or wish to receive your emails again, they can opt back in to your campaigns. You should follow the process detailed in the article below to remove an opt-out:

How can I remove bounced/opt-out emails from my Act! database?: Article ID 37150

How do I import an existing opt-out list in to Act! emarketing[1]?

If you have previously used another emarketing service or have kept a manual list of your opt-outs you can provide them to us in CSV format by contacting Technical Support and we can add them to your account. We will confirm once the opt-outs have been added to your account. You can find out how to contact us in the following articles – use the one for your region.

Where can I find contact information and business hours for United Kingdom customer service and support?: Article ID: 38273

Where can I find contact information and business hours for North American customer service and support?: Article ID: 36696

Although the above will assist you managing opt-outs via emarketing[1], Act! can also be used to allow you to track opt-outs for other methods of contact such as SMS or postal mail. You are able to track this via custom fields in Act!. There are details on creating custom fields and adding them to your layout in the two articles below.

How to create and manage database fields in Act!: Article ID 15335

Designing Layouts in Act!: Article ID: 15332

6.8 Managing opt-outs and opt-ins

Although recipients of emarketing[1] campaigns can unsubscribe and be excluded from your future campaigns you may have to adapt your database to avoid accidental inclusion in a Mail Merge. The workaround for this is to create an additional email field, when sending a Mail Merge or an emarketing[1] campaign Act! will check the default email field. An example of when this may be used is if a customer opts-out of your marketing communication however you may need to keep the customers email address to send them invoices. The custom field can be used to store the customers email address using the functionality within Act! as explained in the following article:

How do I use the Replace, Swap, and Copy options in Act!?: Article ID: 38137

If you use the above method you may wish to start this process by accessing your emarketing[1] opt-outs. You can access your emarketing[1] opt-outs using one of the two methods in the article below dependent on if you are using Act! or Act! emarketing[1]:

How do I create a lookup of my Act! emarketing bounces or opt-outs in Act! v17.2 and later?

How to access your Act! emarketing opt-out list: Article ID 28591

There is more information available on Consent in the following article from the ICO website:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/

6.9 Rights in relation to automated decision making and profiling

The GDPR gives individuals' rights when they are the subject of automated decision making and automated 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 relatively sophisticated technology, please read the detailed information available on the ICO website, here.

Act! 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 the use of Act!. Appropriate notices 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, to enable Act! 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.

The area of Act! that relates to automated decision making is Smart Tasks. It is your responsibility to ensure 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 on Conditions. A customer who has opted-out of your emails could be sent an automated email as part of your Smart Task steps if the information within their Contact record is not up to date.

There are several Smart Task examples available in Act! (though by default these do not run automatically). You can find more information regarding them in the articles below:

What are Smart Tasks in Act!?: Article ID: 37910
How to Create and Manage Smart Tasks in Act!: Answer ID: 26944

7. Accountability and governance

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.

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

Documentation

As part of GDPR, you may be required to produce evidence of your compliance. This can be helped by documenting decisions you have made about using someone's data. Find out more information here.

Act! has a number of features which can help you to record decisions made about the use of personal data:

- Tracking the source of a record within a field
- Attaching supporting documents to a record, such as email correspondence, scanned documents and call recordings.

How to attach a document to a Contact, Group, Company, or Opportunity in Act!: Article ID 17526

- Time stamped note and history data can be recorded against an individual, recording an interaction with them, or marking an internal process which has been followed.

How to use the History List in Act!: Article ID 36109

- Configuring fields to automatically record a history entry when their contents are changed, providing traceability of record changes.

How to create and manage database fields in Act!: Article ID 15335

Act! can help with documenting compliance by providing the ability to store evidence of compliant processing activity. For example a history entry could made by the user, or a file could be stored on the Documents tab, e.g. an archive html page of the appropriate data collection form. This would require user training about compliance requirements and how those requirements affect the use of Act!.

In addition, a user could store internal documentation e.g. Standard Operating Procedures in Act! either as attachments to contact records, or as new menu short cuts for example to individual documents stored externally to Act!.

The following article explains how to create History and also attach a relevant document/file:

How to manually create Histories in Act!: Article ID 38835

Organisations with less than 250 employees must keep records about higher risk processing activities such as processing data which could: result in a risk to rights and freedoms of individuals; or special categories of data; or relating to criminal offences.

Guidelines are available for organisations who need to keep such records and the ICO has indicated that exemptions may be put in place for SMBs. As mentioned above in relation to compliance, Act! may be used to help as a document store in appropriate circumstances.

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

What are custom tables in Act! Premium Plus?: Article ID: 38976

For more information see: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

Codes of conduct and certification schemes

The ICO has a separate section on codes of conduct and certification which gives guidelines on how these may be used by organisations to demonstrate they comply with various elements of the GDPR.

It should be noted that these 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 the ICO's approval of any code of conduct or certification which would be relevant to the use of Act!

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

Each organisation must implement compliance processes, for example documenting compliance and carrying out Impact Assessments. They should also adopt relevant procedures to put in place the measures, to meet the principles of data protection by design and default. Organisations should consult the ICO's website for more information and work with consultants as appropriate to ensure they put in place and maintain the appropriate governance measures.

The following information is provided for information and completeness only. For all the following aspects of GDPR compliance, Act! is most likely to be useful for storing documentation which helps demonstrate compliance with the GDPR, though the section at the end includes information about how Act! can help with processing data relating to children.

8. Appointing a Data Protection Officer

This is required in certain circumstances. Regardless of whether an organisation is obliged to appoint a Data Protection Officer (DPO), s/he must have sufficient skills and resource to comply with GDPR and other relevant privacy obligations. The DPO's minimum required tasks are defined on the ICO website here.

9. 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).

Breach notification

Data processing organisations have an obligation to notify the relevant supervisory organisation of breaches if it is 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. If, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality or other significant economic or social disadvantage. Individuals affected must also be notified when that risk is high.

Notification must be made 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.

You should take steps to educate staff about the notification requirements and put in place relevant measure to identify internal breaches, investigate them and report on them.

Application of GDPR to children

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.

Using Act! CRM 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.

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[2]

1 Act! emarketing servers are located in the USA. We comply with GDPR in transferring personal data to those servers. If using Act! emarketing please ensure you comply with your GDPR requirement to notify your Act! emarketing email recipients that their data will be transferred to the USA. 2 Act! Certified Consultants are third-party vendors. Act! LLC 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