Clear
Software Developers

Get in touch
01257272730
info@clear-software.co.uk

The nature of FirstClass is that it may handle potentially large volumes of personal data, and so compliance with data protection legislation is a very important part of what we do when we develop our products.

Although responsibility for compliance when using FirstClass will always rest with you, we endeavour to make our software operate in such a way as to maximise your ability to operate in a compliant manner. This has included product reviews with specialist data protection solicitors and practitioners to get their input as to how our software can be improved.

We also understand how important it is for us to handle our customer's data responsibly, and so we have set out below some of the ways in which we ensure that you can trust us, and our software, with your personal data.

Features

FirstClass has the following features as standard:

Anonymisation/Pseudonymisation

Anonymisation of records means the removal or alteration of all identifiers so that there is no way of gaining the identity of the data subject concerned. Once personal data has been anonymised, then it is no longer considered to be personal data, and therefore is no longer subject to data protection legislation. For example, you may remove the name of a data subject and then generalise other information so that the individual may no longer be traced.
Any 'identifier' fields also need to be considered to see if they need changing/removing to stop them being used to repopulate the record from the original source.

Pseudonymisation is the process of removing identifiers from the records but retaining the ability to reallocate them by merging such records with other corresponding data. This may include holding the identifiers on a separate database that can then be cross-referenced to complete the records. Pseudonymised records are treated as personal data, and therefore not kept indefinitely, but pseudonymisation creates additional security as further information is needed to identify the data subject.

FirstClass allows the user to configure the anonymisation/pseudonymisation process to carry out the following tasks:

- *On the Person window* - Surname (replacing this with the record ID), Forenames, Initials, Date of Birth and Death (but retains the Year of Birth and Death for reporting purposes), Honorary, Telephone, Fax, Mobile, Email, Occupation (other), Age description, Supporter description, Notes. All aliases and relationships are removed.
- *On the Contact window* - Name (Person Details section), Position, Telephone, Fax, Mobile, Email, Notes
- On the *Person Address window* - Address lines 1 to 4, Town (County, Region and the Postcode district are retained for reporting purposes).
- Once pseudonymised you can no longer edit the above fields (this is to prevent personally identifiable information being accidentally re-entered).

FirstClass can be configured to carry out the tasks above as part of the pseudonymisation routine. This routine is then utilised in two separate areas of the FirstClass system.

- To remove personal information from a number of records you can use the **Bulk Person Pseudonymise** option. This option allows a flat file (.txt or .csv) containing a list of Person ID's to be used to pseudonymise a list of records. The flat file can be generated using a custom report or by exporting data from browsers. Care must be taken when using this option as it is possible to remove large amounts of data from your database!
- A manual option for the user to select an individual person or contact to carry out the pseudonymisation tasks against. This will then pseudonymise the selected person and all of their details.

Deletion

FirstClass has the functionality to permanently delete individual persons or contacts via the system. Related records may need manually deleting first, again through the system, as part of this process to ensure data integrity. Obviously, this feature is only enabled for users with valid security rights.

Review Reminders

Reminders can be set via reviews against a legacy within the system. This could then be used as a reminder to anonymise the data after a certain period of time.

Complete Data Retrieval and Reports on Data Subjects.

Should you need to respond to a subject access request or any other disclosure requirements, FirstClass can easily report on and provide copies of any records. With multiple search criteria this enables you to collate or review the personal data with ease.

Data Encryption

Transparent database encryption can be enabled at the SQL server database level as long as the server edition and version support this. This means the database files and backup files would be encrypted. It would be the responsibility of your IT department to manage your encryption keys.

Installation, Configuration and Support Services

We host your FirstClass data in a UK based secure server facility and as such, we will be considered a data processor and will therefore not only have obligations to you, the data controller, but also to the Information Commissioner's Office and the data subjects themselves.

We are bound to keep records as to the nature of any processing done on your behalf. Usually this is only during installation and configuration services, or where we are providing support to you.

We have adopted good industry practice in securing our own internal networks, and this is regularly reviewed.

We have also adopted best practice if we do require copies of your data, for migration or support reasons, as we will permanently delete this data once it is no longer needed. Occasionally this may mean that we have to ask you to supply us with it again, but we think it is better this than to hold data for longer than necessary.

All our employees have been trained on data protection and are aware of their responsibilities to keep personal data secure.

What you need to be aware of

Whilst we do what we can to help you be compliant, you need to be aware of the following points:

- Responsibility for compliance with data protection legislation remains with you at all times. We have endeavoured to develop our products in such a way as to assist you in your compliance efforts but cannot be held responsible for your use of our products.
- You are responsible for providing data subjects with appropriate information about any data processed by you in respect of them or obtaining consent to such processing if required. All data processing must be transparent, fair and lawful and so whilst our software can be used to store, access and analyse large quantities of personal data, you need to ensure that you have made the data subjects aware of how you will be using any data collected.
- Take care when inputting data into FirstClass as it is highly likely to be considered personal data. Ensure that you meet one or more of the lawful basis's for processing such personal data.
- You should take appropriate legal advice in respect of your obligations under data protection legislation, and where appropriate cyber-security advice from reputable experts.
- The underlying database is held in a UK based secure server facility with ISO 27001 data security accreditation.