eSAFE

How does eSAFE keep your data secure?

Your data is stored by Salesforce on secure servers within Europe and is covered by all relevant European data legislation (GDPR). Standard Salesforce security features include:

Access to the system

All users have unique user names and passwords. Each service can decide on their password requirements. System administrators can see login history of all users, which allows you to track who was logged into the system and when.

If logging from an unknown device, user has to confirm their identity by entering a code sent to their email or mobile phone. From 2022 Salesforce introduces mandatory Multi Factor Authentication, which means that all users will have to approve login request via Salesforce mobile app.

Using the system can also be restricted to specific hours or IP range.

Security profiles

Access to any personal data should be given to authorised staff on a 'need-to-know' basis. Each service can set up different user profiles, determining who should have access to what information (this can be Read, Edit, Write, Create and Delete). System automatically tracks who edited last each record (timestamp and username).

Some fields can also be visible only to certain profiles.

Data retention

eSAFE can ensure that data is anonymised in line with the service policy. Enclude recommends that the System Administrator reviews the data before it's anonymised. Reports can be used to identify records which are no longer required. This will depend on your processes but could be based on Last Modified Date, most recent Intervention or a date the Engagement record is marked inactive.

Please note, that for data to be considered anonymous, it must be impossible for any individual to be identified from the data by any further processing or by combining it with other information. (Related data e.g. Emergency contact)

Accidental loss

You can decide which user profiles can delete different type of data. If data is deleted accidentally, it can be restored by the System Administrator within 10 days. After that time, the only way to restore data is from the backup file.

Data backups

Enclude recommends scheduling weekly data backup. Remember to ensure that the exported file is stored securely. You can find detailed instructions how to do this in Enclude Members' Corner.

Field History Tracking

Salesforce allows you to track changes to up to 20 fields in any object (e.g. Contact, Service Intervention) logging who made changes and when. However, long text field values before and after changes cannot be captured, so this may be of limited value for eSAFE users.

Setup Audit Trail

The System Administrator can review all configuration changes, including security-related changes that have taken place over the last 6 months. It can be useful to archive this log on a regular basis so that if questions arise after 6 months have elapsed the audit trail data is still available.

What can you do to protect data stored in eSAFE?

- Do not share your login details with anyone
- Ensure your data exports are encrypted/password protected. Data exported from Salesforce may be the weak link in your security if exported files are not properly secured. This also applies to exported reports that include personal data.
- Make sure that any printouts from the system are disposed of carefully
- Assign specific responsibility to someone for ensuring that personal information is not retained on eSAFE any longer than necessary