With careful consideration for your requirements, Lokulus can play a key role in your strategy for a General Data Protection Regulation (GDPR) solution.

When designing a solution compliant with the GDPR, of the seven principles that it requires that organisations adhere to six are relevant in this context:

- Fairness and transparency
- Purpose limitation
- Data minimisation
- Data Accuracy
- Data Deletion
- Security

You can be distill these into the following five considerations for the Lokulus platform.

Data Accuracy

Individuals have the right to request what data an organisation has on them, and they have the right to have it deleted. Lokulus allows you to do this very quickly through customer searches and to devise reports of the data.

Customer details are easily managed and deleted (after a fixed retention period) through the archiving and deletion features built into the platform.

Data Archiving and Retention

Lokulus has an archiving tool that will aid you in GDPR compliance. It allows you to configure when you archive data and when it, having exceeded its retention period, is deleted. You can also use the tidy feature to only retain the events on a customer's record relevant to GDPR.

For further details, see the *Archiving and Maintenance* fact sheet.

Data Access Management

With Lokulus, you can define access rights at various levels. An agent might have different rights than their supervisor, and other groups of agents may have additional access rights for different brands.

User access is managed through:

- Users
- Groups
- Profiles

With careful consideration of users and groups, all users need only access the data they require to do their job. See the *Workforce Management* fact sheet.

For example, agents may not need to see the history events associated with the case customer or work item. In which case, you can set up a profile not to include the history events tab. Their supervisor, on the other hand, might have access rights to see the history events.

A typical set of Groups look like this:

Agents	Team Leaders	Content Author
Controller	Administrators	Processor

Data Access Auditing

For auditing access to data Lokulus has the following two features.

Case and Customer History Events

Including any changes and views by users, this information leaves an audit trail of every interaction with customer records, which can be provided on request."

Search Audit

The search audit aids in compliance with data breach notifications. It allows you to see all records searched for and by whom during a particular period.

The information recorded contains the time of the request, the user ID, method and the parameter. This is enough information to replicate the search should a data breach be suspected.

Data Minimisation

To limit the collection of personal information Lokulus have a clear strategy.

- All forms which collect customer information only collect that which is relevant to the business process.
- Personal information is only displayed when it is necessary for the task to be completed.
- Information that doesn't have to be retained is displayed through mix-in processes.

In addition, you can set up tidy tasks that will remove any unnecessary history events, pertaining to the customer's records and delete records once they have exceeded a particular retention time.