Sage CRM and the GDPR

Overview

Updated: March 2022

Contents

About this Guide

This guide explains how the EU General Data Protection Regulation (GDPR) affects you as a user of Sage CRM. For more information about the GDPR, see http://www.gdpr.eu.

Sage Legal Disclaimer

The information contained in this guide is for general guidance purposes only. It should not be taken for, nor is it intended as, legal advice. We would like to stress that there is no substitute for customers making their own detailed investigations or seeking their own legal advice if they are unsure about the implications of the GDPR on their businesses. While we have made every effort to ensure that the information provided on this website is correct and up to date, Sage makes no promises as to completeness or accuracy and the information is delivered on an “as is” basis without any warranties, express or implied. Sage will not accept any liability for errors or omissions and will not be liable for any damage (including, without limitation, damage for loss of business or loss of profits) arising in contract, tort or otherwise from the use of or reliance on this information or from any action or decisions taken as a result of using this information.

The GDPR Overview

The GDPR was designed to harmonize data privacy laws across Europe, to protect and empower all European Union (EU) citizens' data privacy, and to reshape the way organizations across the region approach data privacy. It replaces the Data Protection Directive and the local laws that implemented this directive. It also changes the process that companies outside the EU must follow to properly protect EU citizens' personal data. While this document addresses the requirements of the GDPR, please bear in mind that other laws may also impact individuals' privacy in some countries and we advise you to take further advice in this respect.

The GDPR applies to automated personal data and data held in manual filing systems. The GDPR creates new rights as well as strengthening those under existing laws. Individuals have the following rights.

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

The GDPR will apply from 25 May 2018 to

- Controllers and Processors established within the EU, regardless of whether processing takes place there or not.
- Controllers and Processors that are not established in the European Union, where the processing activities relate to:
  - the offering of goods and services to Data Subjects in the Union, irrespective of whether payment is required.
  - the monitoring of the behavior of European Union Data Subjects where the behavior takes place in the European Union.

Personal Data

Personal data is any information that could be used to identify an individual directly or indirectly.

Personal data generally includes names, addresses, phone numbers, email addresses, salary, performance ratings, credit card and bank details, payment records and similar information. It also includes online location identifiers and IP addresses, expressions of opinion about an individual, and any indication of intentions towards that individual.

Sensitive personal data is more strictly controlled in data protection legislation. Article 9 of the GDPR defines sensitive personal data (“special categories of personal data”) as follows.

“Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.”

This definition may be extended by local laws.

Standard personal data fields in Sage CRM include Person First Name, Person Last Name, Person Email Address, Person Phone Number (Business/Mobile) and (particularly in a Business to Consumer environment) Person Address. This list is not exhaustive. Because Sage CRM is customizable, you can add custom personal data fields to Sage CRM such as National Insurance Number or extend standard Sage CRM fields to capture personal data.

Sage CRM and the GDPR

Sage CRM features can help you meet your GDPR obligations regarding personal data held in your Sage CRM system. It is important to consider data held in other systems, spreadsheets, and printed records to understand your full GDPR obligations.

The following is a non-exhaustive list of GDPR requirements.

- Requirement 1: Securing data
- Requirement 2: Managing data
- Requirement 3: Retrieving data

Requirement 1: Securing data

Installing Sage CRM

Sage recommends that Sage CRM is installed in line with good security practices which may include using a firewall, and implementing server and database security measures.

For more information, see

- Installing a secure system
- Configuring proxy settings
- Setting a custom server name for internal requests

Backing up data

Establish a comprehensive data protection plan that includes mirrors, snapshots, replication, and secure backups. Consider any personal data stored in backups as part of your GDPR processes, especially when considering erasing data that can no longer be retained.

- Limit the role of the person who performs backups.
- Perform backups regularly and frequently.
- Perform test restores of backups.
- Centralize and automate backup management.
- Document all backup tasks.
- Review backup logs daily.
- Encrypt backups.
- Protect the backup database and catalog.
- Use remote storage or Cloud storage.
- Store backups on RAID arrays.
- Stack your backup solutions.
- Ensure backup is part of your change control process.

Controlling access to data

Ensure that access to personal data is managed correctly to meet the data security requirements of the GDPR. Sage CRM lets the system administrator limit data access by configuring user roles, user templates, security profiles, and security policies. For example, your administrator can segment your customer data by geographic territory, so a user who's responsible for customers in one country sees customer data for that country only.

For more information, see

- Configuring a secure system
- User templates
- Working with field security
- Security management
- Required security profile rights

Enabling third-party integrations

If you've enabled the Sage CRM and MailChimp integration, review your contract with MailChimp to understand where data is held and your responsibilities as a user of the service. If you anonymise data in Sage CRM, manually delete contact personal data from the contact lists that you provide to MailChimp. For more information, see Deleting personal data.

Creating an audit trail

Maintain an audit trail of any edits to personal data using tracking on Lead and Opportunity records.

Requirement 2: Managing data

Monitoring personal data

Monitor and manage all personal data that your company collects. First, identify personal data and then verify that you need it.

1. Identify the Personal Data that your company collects, if you are unsure what data is personal under the GDPR, look at guidance from your local regulatory authority such as the UK's Information Commission Office or seek appropriate expert advice. Remember to include any custom fields or entities you've created in Sage CRM to capture personal data.
2. Review the length of time you keep personal data. You can run a report to find personal data in Sage CRM that's older than your required retention period. For more information, see Creating a report. You can also create a notification that reminds users to reobtain consent or delete personal data after a specific date. For more information, see Creating a quick notification.
3. Consider the reason why you collect personal data when deciding whether, and for how long, you retain it.
4. If a contact does not respond to a consent email or withdraws their consent, exclude them from future e-marketing emails. To do this, include consented contacts only in the Sage CRM group for the campaign.
5. Identify data that has been shared with Mailchimp. You can run a report to find all records for which the **This record was sent to** checkbox was selected. For more information, see Creating a report.
6. Consider scenarios where you may receive the data again when specifying the date on which you review the data.
7. Identify data that your company no longer needs or is out of date.
8. Create an escalation rule that uses the creation date, last modified date, and bespoke date fields to indicate personal data to be reviewed and deleted, and to indicate where data has been shared with a third party. For more information, see Creating an escalation rule.

Deleting personal data

Securely delete personal data that is no longer needed, and update, archive or securely delete personal data that is out of date.

1. Use mass update to hide personal data from all marketing lists and make the data anonymous. For more information, see Performing mass operations.
2. Delete personal data, and all related documents and communications. For more information, see
   - Deleting all documents for a person.
   - Deleting all communications for a person.
   - Deleting all communications for a lead.

- Mass deleting communications.

3. If your company has shared personal data with MailChimp, manually delete or supress this data. For more information, see Checking if a Person or Company record was sent to MailChimp.

Requirement 3: Retrieving data

1. Create a Subject Access Request (SAR) template to be used whenever a customer wants to review personal data. For more information, see Creating a template using the text editor.
2. Run a report to retrieve requested information. For more information, see Creating a report.
3. Record the following information for each SAR. Your system administrator can create a custom entity to record this information and link it to the relevant personal data records. For more information, see Creating a custom entity. Alternatively, you can record this manually outside Sage CRM.
    - The individual who submitted the request.
    - The date on which the customer ID was verified.
    - The request date.
    - The date the request was completed.
    - The output report.
4. Complete the SAR template and email it to the customer. Save the SAR as a communication linked to the relevant Person record in Sage CRM.
5. Update data if a customer notifies you that it's incorrect or has changed. For more information, see Customer information. Save a scanned copy of the letter or email requesting the data change linked to the relevant Person record in Sage CRM. You might have a process in place to store this information externally to Sage CRM.

Integrations

If your Sage CRM system is integrated with another Sage product or linked to a Sage Back Office product, personal data might remain even if you anonymize it in Sage CRM. It is your responsibility to understand what happens to data in the other product and to anonymize or delete data in the other system.

If a customer submits a right to be forgotten request, ensure it is performed in both systems, unless regulations require preserving data for compliance or other reasons.