General Data Protection Regulation (GDPR)
A Practical Guide for SmartSimple Customers

Version 1.1 (Rev. May 8, 2018)

This document assumes the reader has a working knowledge of the SmartSimple Process Automation Platform.

Disclaimer: This Guide does not constitute or substitute legal advice. If you have any questions about the content of your data policies, please consult a legal professional. This Guide will also be periodically updated to reflect the evolving nature of the privacy and data protection landscape.

Introduction

The European Union's General Data Protection Regulation (GDPR) comes into force May 25th, 2018. It represents a new gold standard in data protection and privacy laws. And with the current scandals engulfing companies such as Facebook, we can anticipate similar legislations coming to other jurisdictions over the next few years. So let's get ahead of the story!

GDPR is providing lots of opportunities for the legal profession with all kinds of agreements required to support the relationships between parties, but this document is not going to talk about anything legal. Rather, we are going to describe practical configuration changes you can make to your SmartSimple system to support this legislation.

Fortunately, we have been adding features to the SmartSimple platform for the last couple years that can be easily used to support GDPR and provide the high auditability and transparency standards required.

Data Categories and Policies

The first step you will need to take is to define the categories related to the data you are holding. This part of the discussion usually happens offline, and can involve other people in your organization such as a Privacy Officer, Compliance staff or other members of the executive team or even the board.

If your organization is large, you probably have a data categorization model in place, and you should use that model.

In the simplest possible scenario, you will have personal information and non-personal information.

Turning your policies into SmartSimple configuration is simple as you can use the Global Settings, Security, and Data Categories to establish this categorization within the system.

Using this feature, you establish each of the categories that you require.

For example, you may have a data categorization model that includes Personal Information, Confidential, Secret, etc. Remember your categories can encompass all type of data categorization beyond GDPR.

- Each category is linked to one or more policy that you define.
- Each category is also liked to the actual data fields in the system that fall into that category.

Pseudonymization

An important feature of Data Category is the ability to use Pseudonymization. Pseudonymization provides the ability to anonymize a field value to the user through the use of a mask.

The data mask describes how much of the field value should be masked from the user. If a field value is anticipated to be 11 characters and the mask length is set to 9 then only the last two characters of the value would be displayed.

Field Value (11 characters)	67828392898
Masked (9 characters)	*********98

Policies

Policies define the way you need to manage the data in a category. Typically there will be two policies for each category.

- Retention policy – defining how long your organization will need to retain the data of this category in the system before it is erased.
- Security policy – defining who can see and/or modify the data of this category in the system. Security policies support SmartSimple Role-Based security.

After you have set up the categories and policies, you then attach the fields to each category. Once the fields are connected to the category, the security will become effective.

More about Retention Policies

Retention is based on a number of months or days after a specific date. That date is part of some other system object such as a grant application process.

For example, if grant application requests the grant seeker must enter a Social Insurance Number (SIN), then a retention policy can specify that the SIN number should be erased one month after the application submission date. In this example, the application submission date is simply a field on the grant application.

- Erasing information based on retention policies is fully automated and takes place nightly.
- The data is not simply blanked out but rather the value ******* is written over the existing value.
- The policy also lets you control if the audit log for the field value should also be erased (i.e., all the field value changes up to the erased data).

Once you have completed setting up the categories and policies, you are on your way towards a GDPR compliant system.

The next sets of configuration changes you need to make are related to the end user understanding what you are going to do with the data and how they can exercise their rights.

Flagging Personal Information Fields

It's essential that the end user understands why you are asking for personal information and what you plan to do with that data.

We support this requirement by giving you the ability to indicate any field that will hold personal information and provide you with the ability to set a description of the uses for that field. Though this feature can be used independently of Categories and Policies, it's best when all these features are used together.

When the user displays any page in the system that uses personal information fields, they have the ability to see all the explanations you have added.

All fields in the system (both standard and custom) can be tagged in this manner, so it does not matter which objects the fields are associated with: users, roles, Universal Tracking Applications, activities or transactions.

When you display the custom or standard field setting, you will notice setting 'Enable as Personal Data' options when you select this option you are required to provide a description.

Auto Erase Contact Details

In order to comply with the Right to be Forgotten clause of GDPR, a new feature has been added – Erase this contact.

The feature is controlled through a button on the contact profile caption erase this profile. When you click this button the following actions are taken:

- A warning is displayed to the user that this action cannot be undone and that some data cannot be deleted such as scanned images containing personal information, generated PDFs containing personal information.
- All the fields in the user profile are set to the numeric system user id including first name, last name, email address, address fields, attached documents are deleted. The deleted values are erased and will not be recoverable.
- This action is logged and the log stores the user that initiated the action and the ID of the contact being erased.

- A Certificate of Erasure is generated.
- Once the profile is anonymized, the button that was used to trigger the process now displayed the Certificate of Erasure with a print and email option.

Use of Global Search to Validate Contact Removal

We recommend that you use the Global Search feature to ensure that all references to the contact have been deleted from the system by providing searching of all fields and indexed documents in a single search.

- This feature is enabled through Global Setting.
- Once enabled you need to associate this feature with one or more roles.
- The Global Search will be displayed under the main menu, Tools sub-menu.

Privacy and Security Policies

The next feature we are going to review is how you can use the Privacy and Security setting page to show end users what their rights are under GDPR. You can access the Privacy and Security Policies Using the Global Settings, Security tab.

Traditionally these settings were used to describe how your organization would manage an end user's data but in the context of GDPR, you should use these settings to describe the user's rights.

- Right of Access.
- Right to Rectification.
- Right to Erasure.
- Right to Restriction of Processing.
- Notification obligation regarding rectification or erasure of personal data or restriction of processing.
- Right to Data Portability.
- Right to Object.
- Automated individual decision-making, including profiling.

Here is what you need to do:

1. Set each of the existing policy types to the GDPR rights. You will find the content of the right in the appendix to this guide.
2. The introduction text needs to be specified as related to GDPR.
3. Use the Global Setting, Language Library to changes the caption Policies to Your rights.

Forcing End User Agreement

You can force the end user to accept each of these at login by setting the Force Acceptance Date and setting the associated date.

In addition to the user having to accept the policies the system will generate a PDF of the signed document with a date/time stamp.

Now any end user will be able to access the GDPR rights definitions right from within the system.

GDPR Request Tracker

Now that you have re-configured SmartSimple to meet GPPR requirements one final optional step is to provide end users with the ability for end users to inform you that they want to exercise their rights.

You will need to establish internal processes to manage these requests, but you can easily gather these requests through the use of a new UTA – the GDPR Tracker.

We won't go into too much detail on the configuration of this UTA but it will end up being lined with "Your Rights" as shown below.

For more details contact our GDPR Technical Analyst at GDPR@smartsimple.com

Reporting Functionality

We have added all the settings and objects we have discussed to the SmartSimple Reporting system. So you can create reports on:

1. Categories
2. Policies
3. Fields
4. Personal Information designated fields

Summary

When you decided to go with SmartSimple as your platform GDPR was probably not on anyone's radar but now it is, and it is truly a big issue. Fortunately, you did choose SmartSimple, and our approach to system architecture has made it relatively easy for us to make sure you can support the legislation.

Making these changes will put your organization in an excellent position as related to GDPR legislation.