CiviCRM and GDPR

VEDA
CONSULTING

Parvez Saleh
V1.3
17th January 2018

Overview

This document is intended to provide an overview to the GDPR guidelines that affect CiviCRM and the charities that use the software.

About Us

Veda NFP Consulting provides consultancy and development services for Not For Profit businesses around CiviCRM and related technologies, such as Drupal, Wordpress and Joomla. We provide services in all stages of project lifecycles, from business analysis through to implementation and support. We are dedicated to the Not For Profit sector and have strong understanding business needs in this arena. We are responsible for implementing one of the largest UK CiviCRM installations at Bloodwise, formally Leukaemia & Lymphoma Research. We are also regularly contribute to the CiviCRM community by developing and releasing extensions.

Introduction

CiviCRM is specifically built for the Not-For-Profit sector and comes with a vast number of functions that can be leveraged to help with donor engagement. Unlike closed source systems, such as Razors Edge, you do not have to pay any fees to turn on additional functionality. Also you are not paying a per user license as you would with a software as a service solution such as Salesforce.

Further statistics can be found at https://stats.civicrm.org

CiviCRM is an open source solution, unlike proprietary software, Open source software is crowd developed and therefore has a far larger pool of resource and support. More importantly with respect to issues such as GDPR the larger pool of resource allows the product to react quickly to new requirements. This was demonstrated during the move to online Gift Aid submissions, CiviCRM was the first major fundraising software to be ready for HMRC's new online system at the time. The added benefit was that the functionality became available to all installs of CiviCRM immediately without cost and we would expect the GDPR work to be tackled in the same fashion, with thousands of charities benefitting from the collaborative model.

Specific to GDPR, CiviCRM is normally deployed with supporter facing interactions, ensuring that any changes to communication preferences are reflected immediately within the database and therefore reduces the risk of communicating with supporters who have requested opt out, from the channel, group or any combination thereof. The GDPR directives have highlighted the need for security and best practise to also be considered in the overall compliance, therefore the following sections of the document detail the approach that Veda NFP consulting will be taking as well as some core enhancements to CiviCRM to ensure GDPR compliance is achievable in all scenarios.

Our role is to guide our clients through the best practises and follow our planned implementation roadmap over the coming 6 months. The GDPR guidelines do require clarification in some areas, however we feel there is enough information to begin the process, reaching the final industry agreed best practise in time for the May 2018 implementation deadline.

GDPR Extension

Our new extension aims to enable charities/organisations to manage their supporters in a GDPR compliant manner. GDPR in itself does not introduce many new requirements however it does introduce a number of new obligations on organisations that hold and use data about individuals.

It’s important to understand that simply moving to an opt in process and regarding all existing contacts as being opted out overnight is probably not what is best for your organisation. There are many factors to consider before determining whether to base your marketing contacts on an opt in . For example a membership organisation is likely to be well within its rights to base member communications on the organisation’s ‘legitimate interests’ unless the member explicitly opts out. You may also be able to import contacts from third party fundraising systems, where they have already stated that they are happy to be contacted by the charity they are fundraising for. The overall aim of this extension is to help organisations navigate the journey to GDPR compliance without compromising their presence with and income from their existing supporters.

Under GDPR, therefore, you need to be able to record whether your contacts have given consent to receive marketing. If so, you must be able to show who consented, when they consented, how the consent was given, and exactly what the consent is for (including for which communications channel – post, email or phone, for example).

If you have not asked them to provide consent, your marketing would be based on ‘legitimate interests’. In this case you must record any contact from them asking not to receive marketing, or specifying which marketing they do not want to receive. You should also be able to show that your legitimate interests are not outweighed by their interests. If people don’t respond to your communications over a period of time, the longer this goes on, the harder it might be to argue that you still have a legitimate interest in contacting them.

More details about GDPR and CiviCRM can be found at https://vedaconsulting.co.uk/GDPR

The current version of this extension does the following;

- Allow you to record the data protection officer for your organisation
- A new tab 'GDPR' in contact summary will display group subscription log for the contact
- Custom search 'Search Group Subscription by Date Range' which can be access from GDPR Dashboard
- Access list of contacts who have not had any activity for a set period of days from GDPR Dashboard
- Ability to force acceptance of data policy/terms and conditions when a contact logs in and recording this as an activity against the contact with a copy of the terms and conditions agreed to. This is currently Drupal specific.
- The right to be forgotten, allowing users of CivicRM to easily anonymise a contact record, hiding any person details but keeping the financial and other history. The action also exists as an API and therefore can be bolted into other processes.

Future releases will include

- User friendly communication preferences, moving to explicitly worded opt in mechanisms.
- Communication preference to include medium per group. Currently CiviCRM supports include or exclude from a group but it does not allow for the selection of the communication medium that should be used for example happy to receive email newsletters but please don't send me any other emails.
- Recording audit information when a contact is exported
- Allowing all exports to be produced with passwords if produced with the MS Excel Extension.

GDPR comes into force in the UK on May 2018, we aim to complete the feature set of this extension by Feb 2018 and if you'd like to get involved please do feel to get in touch. We'd also like to take this opportunity to thank Paul Ticher (http://www.paulticher.com/data-protection) for coming on board with this project as a consultant and expert in the sector.

Other GDPR related practises

The following is a guide for practises we will be putting into place on all clients hosted with us, as mentioned these are not directly GDPR specific but aimed at producing a best efforts guide for CiviCRM users.

Audit of communication preferences

CiviCRM has an extensive logging and audit setup, ensuring every change in the database can be reviewed. The GDPR guidelines require that the opt in and out are available to the supporter and that the charity can see these options.

Currently CiviCRM has two forms of opt in/out. Firstly, in the communication preferences, supporters are able to indicate if they consent to being communicated to via marketing channels. Secondly, supporters are able to indicate specific marketing communications using subscriptions to groups. These two methods ensure that compliance of opt in is met when communicating with supporters.

Linking Scheduled reminders to comms preferences

At present CiviCRM workflow based emails, such as donor journey emails, do not have an opt out mechanism. For example if a supporter donates and CiviCRM has been setup to send 1 week, 1 month and 6 month emails, then the email content does not need to include opt out links in order for CiviCRM to send the email chain. In order to comply with GDPR directives CiviCRM needs to include the ability to opt out of chained emails. In order for organisations to get the most from the chained emails whilst including the ability for supporters to opt out, we will be adding extra opt out options to include workflow chained emails. This method ensures that a user can opt out of chained communications without having to globally opt out of all communications.

A new extension will be developed and delivered in order to ensure this functionality is available in CiviCRM. We're expecting to complete this work in January 2018.

Two Factor Authentication

With standard security procedures (especially online), by only requiring a simple username and password, it has become increasingly easy for criminals (either in organised gangs or working alone) to gain access to a user's private data such as personal and financial details and then use that information to commit fraudulent acts, generally of a financial nature.

Two Factor Authentication, also known as 2FA, two step verification or TFA (as an acronym), is an extra layer of security that is known as "multi factor authentication" that requires not only a password and username but also something that only, and only, that user has on them, i.e. a piece of information only they should know or have immediately to hand - such as a physical token.

Veda NFP Consulting will be implementing 2FA for all of its hosted clients by October 2017, with implementation schedules being shared by August 2017.

Introducing 2 Factor Authorisation and Google Authenticator

- Two Factor Authentication, also known as 2FA, two step verification or TFA (as an acronym), is an extra layer of security that is known as "multi factor authentication" that requires not only a password and username but also something that only a user has on them, i.e. a piece of information only they should know or have immediately to hand

- Google Authenticator is an application that implements two-step verification services using the Time-based One-time Password Algorithm (TOTP) and HMAC-based One-time Password Algorithm (HOTP).
- The Authenticator provides a six digit one-time password which users must provide in addition to their username and password to log into applications or websites.
- A user installs the Authenticator app on a smartphone, ipad or tablet. To log into an application or service that uses two-factor authentication, the user provides a username and password to the site and runs the Authenticator app. The app displays an additional six-digit one-time password; the user enters it, thus authenticating the user's identity.
- For this to work, a set-up operation has to be performed ahead of time: the site provides a shared secret key to the user over a secure channel, to be stored in the Authenticator app. This secret key will be used for all future logins to the site
- With this kind of two-factor authentication, mere knowledge of a username and password is not sufficient to break into a user's account. An attacker also needs knowledge of the shared secret key or physical access to the device running the Authenticator app.

User Session management

Along the lines of the 2FA approach, we feel that a potential weakness in security is users leaving their logged in computers unattended or failing to logout/close browser. This could allow unauthorised access to data. In order to minimise this risk we will be reducing the amount of time a logged in session remains active in CiviCRM whilst being inactive.

In order to minimise the risk of unattended or previously logged in sessions we will be introducing a shorter session timeouts on a per client basis i.e. after 15 minutes of inactivity the user will need to login in order to access CiviCRM.

We would also encourage charities to ensure their user operating systems are setup with the appropriate level of idle locking, requiring a password to re-enable access and disabling the option to save passwords in browsers.

Weak Passwords

Users often use the same password across several systems and therefore compromises in external systems could leave the CiviCRM user record vulnerable to abuse. We will be introducing password expiry systems, forcing all users to reset their passwords within a certain period of time on a per client basis.

Backups

In order to protect clients data and ensure integrity backups are kept in at least two locations.

The first is on the server that the CiviCRM is hosted. The second is using Amazon Web Services S3 backups. This ensures that if the hosting server is compromised in any way, including hardware failure, the backups are available offsite. The backup cycle is as follows.

- Daily - Every night, kept for 14 nights
- Weekly - Every Sunday, kept for 8 weeks
- Monthly - First week of every month, kept for 12 months

Encryption of the Databases

One of the techniques the GDPR directives encourage for mitigating risk is to ensure that databases are encrypted. All Veda NFP Consulting installations are always setup to access via HTTPS protocols, ensuring data transmission between the clients machine and the server are encrypted, as any commerce site would be.

A further level of encryption that we'll be bringing online over the next 6 months is to move to MariaDB 10.2+ from MySQL. The key benefit being that MariaDB 10.2+ supports encryption at rest. The added benefit being that a clone of the database due to server access would make it unreadable on another server.

We expect to complete the rollout of this process over the next 6 months, each client will be informed of their individual migration plans.