CiviCRM and GDPR

VEDA
CONSULTING

Parvez Saleh
v1.2

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 are a software consultancy company who specialise in CiviCRM, responsible for implementing one of the largest UK CiviCRM installations at Bloodwise, formally Leukaemia & Lymphoma Research.

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

The General Data Protection Regulation (GDPR) enables individuals to better control their personal data. It is hoped that these modernised and unified rules will allow businesses to make the most of the opportunities of the Digital Single Market by reducing regulation and benefiting from reinforced consumer trust.

The Data Protection Directive: The police and criminal justice sectors will ensure that the data of victims, witnesses and suspects of crimes, are duly protected in the context of a criminal investigation or a law enforcement action. At the same time, more harmonised laws will also facilitate cross-border cooperation of police or prosecutors to combat crime and terrorism more effectively across Europe.

The GDPR was ratified by mid 2016 and immediately became law. Member states now have a 2 year implementation period. Enforcement will commence by May 2018 at the latest.

Veda NFP Consulting are putting in place a guideline to help charities remain GDPR compliant. This guideline is in no way the sole requirements for GDPR compliance and charities should take steps to ensure they are following all the directives set out.

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.

The CiviCRM community, including Veda NFP Consulting, are producing a GDPR communications extensions that will ensure the changes to the communication preferences also result in activity records being created with the details specified in the GDPR guidelines, namely ensuring the following GDPR directives are met;

- Send a follow up email to all engaged data to ask them to opt-in to continuous communications based on the assumption that all previously obtained consent may be based on the optional opt out model
- Right to be forgotten, anonymising a contact without losing engagement history
- Allow charities to produce clear consent history to 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 globallly 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.

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.