Data Security within our Applications

Overview

Our integration applications move data between different sources and destinations. Some usage data is transmitted to our servers. This article outlines where data is moved and stored and what security is in place to ensure that data is protected.

The article applies to all of our applications. However it is perhaps more relevant to those applications that transmit data between Raiser's Edge and other third parties such as MailChimp (in the case of Chimpegration) and other data sources e.g. Eventbrite, iSAMS, Crowdrise, Classy, etc in the case of Importacular. For simplicity sake we will refer to all of these third party sources of data as "data sources"

Data Storage

Data is typically stored within Raiser's Edge or with the data source. All biographical, address, phone, email and gift data is either stored in Raiser's Edge or in the corresponding fields in the data source. At no time is any of this data ever moved to a third party or does it pass through a third party. At no time does Zeidman Development ever receive any of this data.

The only time that we will ever receive any of this data is if you send it to us directly. This may be useful for troubleshooting a problem. This will only ever happen if you initiate it and send it to us via email or some other means. There are no automated troubleshooting processes in our

applications. We understand your data protection concerns and will gladly sign a non-disclosure document if we need some data to troubleshoot.

Any data that is held is either held within Raiser's Edge or the data source. Your organisation may be hosted by Blackbaud in which case they will store your data and data will pass from the Blackbaud hosting environment to the data source.

As mentioned earlier our applications do communicate with our web services. They send activation details to ensure that your licence is still valid. They also send aggregated statistics about which Importacular data sources you have been using. This helps us to focus our attentions on the most commonly used data sources and make improvements to those that are utilised the most. This is the extent of the data that the application transmit back to Zeidman Development.

Transmission

Whenever data is transmitted to a data source from Raiser's Edge or to Zeidman Development the applications use SSL i.e. they connect using the https protocol. This is the same connection that you would use when connecting to any secure site e.g. banks. It offers the highest level of security. We rely on our partners, the data sources and Blackbaud to ensure that when the receive the data via https that their website and APIs have valid security certificates. If they do not then the transmission will fail so that no data will be sent.

In one case we transmitted the data via SFTP. This is Secure File Transfer Protocol and it is the equivalent data transmission protocol but specifically for files. Again this relies on a security certificate to ensure that the data is transmitted sucessfully.