Redkite Data Protection and Privacy Statement

March 2018

Version Control

Date	Version No.	By whom
28 November 2017	1.0	D. Arber
09 January 2018	1.1	D. Arber
30 March 2018	1.2	D. Arber

Table of Contents

1. Purpose

1.1 We take the privacy and security of your information very seriously and have adopted security measures both within the physical environment in which your information is stored and within the applications to ensure that your information is protected.

1.2 The purpose of this document is to outline what Redkite Systems is doing to meet the requirements of GDPR.

2. Assumptions

2.1 This document assumes that, for our hosted customers, that you, the customer, are defined as the 'Data Controller' and we, as your supplier are defined as 'Data Processor'.

2.2 For non-hosted customers, that you, the customer, are defined as 'Data Controller" but also take on some responsibilities (highlighted with an *) from the list of responsibilities detailed below for the Data Processor.

2.3 That we agree that there is no specific technical requirement for system security in GDPR and that the data processing and security requirements are based on risk, the nature of the information stored within the system, and the purpose for which the information is processed together with other factors, and on that basis, we are confident that the security we have in place for our hosted customers is of a very high standard and is more than proportionate.

3. Roles

3.1 Data Controller

3.1.1 The function of the data controller is:

- to collect the personal data in the first place and provide the legal or other basis for doing so
- to determine which items of personal data to collect, i.e. the content of the data
- to determine the purpose or purposes the data are to be used for - i.e. managing training
- to determine which individuals to collect data about - i.e. fire personnel
- to determine whether to disclose the data, and if so, who to – i.e. line managers and trainers
- to determine what access levels and other rights apply to each user - i.e. the access rights individuals have and the application of these rights through the system tools
- determine how long to retain the data
- how frequently amendments will be made to the data

These are things that can only be done by the data controller.

3.2 Data Processor

3.2.1 The function of the data processor is to determine:

- what IT systems are used collect personal data *
- how to store the personal data *
- to ensure that the security surrounding the personal data is adequate and proportionate*
- the means and security applied when transferring the personal data from servers to the customer *
- the method for ensuring a retention schedule is adhered to, and
- the means used to delete or dispose of the data both during the term of the contract and upon termination of the contract.

4. IT systems and the security surrounding your personal data

4.1 We provide an optional free web hosting service for our customers which provides the level of security and data protection we deem necessary to secure your data and prevent any data breaches. If you are concerned about this level of security, we can help you re-locate your applications and data on to your own servers.

4.2 Your applications and data are held on a dedicated, secure server which is hosted in a secure data centre managed by Rackspace plc who manage our hosted servers and services.

4.3 No data is held on our premises.

4.4 Rackspace plc. hold ISO 27001: 2013 together with other security certificates and policies and we are satisfied that, working with Rackspace plc., we take all reasonable measures to protect your data.

4.5 Rackspace plc. undertake a daily differential and a weekly full back up of your data. Data is held at two data centres; the primary data centre and a second separate secure data centre also managed by Rackspace plc.

4.6 Data is transferred between centres by disc and offsite backups are encrypted with 256-bit AES encryption prior to leaving the primary data centre. Back-up data is retained for 28 days. Data can be restored from these back-ups on request during the retention period.

4.7 All data is transferred from our servers to you via the internet. All data is encrypted during transit between the secure hosted server and your browsers using https:// protected by Thawte 128bit (256bit browser dependent) SSL. (Look for the locked padlock on your screen.)

4.8 Data is retrieved from the system by users via each application and access to the information can be restricted by yourselves using tools available on the system. Access to the information is protected by a user name and password. It is the responsibility of the customer to ensure that passwords are robust.

5. Minimalization of data and type of data processed

5.1 The latest data protection legislation (GDPR) requires that both the data controller and data processor keep personal data held on systems to the minimum.

5.2 The Redkite applications only requires the following minimum information to function:

- A unique ID number – this does not have to be a works or other identifiable number
- First name and Family name (the first name can be an initial)
- The individuals place of work (i.e. the airport or station at which they are based)
- Their department (where the license is for multiple departments)
- Their shift or watch
- Their employment status (optional) e.g. whole time, part time, etc.
- Their role (as defined in CAA CAP 699, where applicable, or as defined within other documents)
- Their rank (where applicable)
- An optional internal email address for notifications.

5.3 All other information is superfluous and should not be held on the system.

5.4 Redkite Systems is offering to physically remove any surplus information from your systems, on request.

5.5 Control measures currently available in the Tracker Editors are:

5.5.1 you can switch off your ability to capture and store additional personal details.

The capturing of additional personal details was included on the system because previously there was a mandatory requirement from the UK CAA to store additional personal information. This information included date of birth, gender, start date of employment, address, next of kin details and next medical due date (without any specific medical information) and ethnicity. Capturing this data is no longer a requirement and the data should be removed from your system. If you require help with the removal, then please contact us.

5.5.2 applying strong passwords

It is your responsibility to protect the access to personal information through the user interface and you can apply certain rules to ensure secure passwords are used on the system. These tools are found in the Tracker Editors / System options / Other menu.

6. Deleting personal information

6.1 Redkite Systems do not automatically delete any data, including personal information, from the system. Due to the way the various system modules integrate and the mandatory need to retain information in different modules for varying lengths of time, it is not technically possible. As the data controller, you will need to manage this - possibly by using the methods described below.

6.2 You can “withdraw” a person from the system via the system editors. You can also set the option ‘Exclude withdrawn people from the system completely” to YES. Once this is set, only the system administrator can see

this person's withdrawn record through the Tracker Editors and the records will not show up anywhere on the system.

6.3 We recommend that you put leavers into folders marked, for example "Leavers 2018", Leavers 2019", etc. It is then quite straightforward to go into that folder and delete the leavers in that folder once the necessary retention period(s) expire.

6.4 Once you delete the person, the records will be permanently removed from the operational system.

6.5 You have a 21-day period in which to notify us of any records deleted in error as these can be restored from back-up during that time. After this time the data will be permanently removed from back-up discs.

6.6 On non-hosted servers you will need to remove the records from any back-ups yourselves.

7. Deleting or Return of data on termination of our agreement

7.1 On termination of your agreement with us your data will be returned to you as a SQL Server database, if requested, and / or deleted from our server. After 28 days the information will also be removed from any back-ups and the information cannot be recovered.

8. Notification of Personal Data Breach

8.1 We will notify our customers of any Personal Data Breach within 24 hours or the next working day from when we become aware of the Breach.

8.2 We will notify you of the nature of the Breach within a further 24 hours (or the next working day) and we will include what categories of information and approximate numbers of Data Subjects and Protected Data Records that have been affected.

9. Transfer of information outside the UK

9.1 All data is held in two secure data centres in London, England. Your data will not be moved outside of the UK.

10. Written permission to hold and process your data

10.1 Under the GDPR you are required to give written permission to us to store and process your data. To this end we have prepared a 'Hosted Data Usage Authorisation Agreement' which will outline the ways in which Redkite Systems can and will use your data. This form can also be found on the web site under Free Hosting.

10.2 Please read and sign the Hosted Data Usage Authorisation Agreement. Once received, we will sign and send back a copy for your records. Electronic signatures are acceptable.

10.3 If you would prefer to use a different form then please send your data protection form for us to review and sign.