Exacom GDPR Statement

Exacom. Preparations for the GDPR, coming into force in May 2018.

In the main the data that Exacom handles on behalf of the license user is in the public domain. However there are a few sensitive areas that we handle such as: Names, email addresses, addresses, telephone numbers and related correspondence that contain personal data. This data will need to be protected while it is in use and eventually it will have to be removed or redacted (documents only) by the license user under the new regulation requirements.

NGRTRPD: From the point when the license user has **No Good Reason To Retain Personal Data.** This is the point when the license user will want to remove personal data from the software and remove or redact any related correspondence that contains personal data, but retain the rest of the application data for future reporting.

The general consensus from our license users is that they would like to retain the historic application data for reporting, beyond the time of NGRTRPD, but concede that the personal data will have to be removed and replaced with a standard set of placeholder data. We are planning to review our current platform to ensure that the personal data fields mentioned above will be encrypted at rest to protect personal data from any theft of data. We are also going to introduce functionality to allow users to remove the sensitive data fields and redact or remove related correspondence from the point when the license user has **NGRTRPD**.

Data in Transit and Backup data.

Currently all data in transit in and out of Exacom and backup data is, and will continue to be encrypted.

Backup data from the time of there is NGRTRPD.

Backup data is more problematic under the GDPR regulations, in that backups include bulk application details and it is therefore almost impossible to delete individual application data from from a stored back up file. This would be laborious and costly to the license user. We have considered the nature of the data that we handle and consider this to be a low risk GDPR area. The backups will cycle over and be over written within a month of being created. Any application data that has been deleted or redacted, will also disappear from any backup media within a month.