

Rooks Move
Data Policy and Processes for GDPR Compliance
Feb 2018

Introduction & Definitions:

Rooks Move is a sole-trading operation owned and run exclusively by Ian Straughan, known as Rooks Move for all trading purposes. Rooks Move is an IT Support & Repair business that also operates Cloud based technologies for and on behalf its customers working solely in the United Kingdom. Rooks Move also conducts Security Audits for its customers when requested.

Rooks Move (Ian Straughan) is registered with the Information Commissioner's Office (ICO) under the Data Protection Act 1988 (DPA), registration number: ZA285226

Data Control & Processing

Rooks Move is both controller of its own data & customer data and data processor of data controlled by different customers.

All data held by Rooks Move on behalf of customers is handled in accordance with all current UK Legislation. This document complies with the UK adopted EU's GDPR legislation which comes into force on 25 May 2018 in UK and Europe.

Data processed and controlled by Rooks Move on behalf of a customer remains the customer's data and will only ever be used with the customer's permission and for their business purposes. Unless the customer expressly requests that Rooks Move continue to store this data for them or is part of continuing work, when the purpose for which the data was stored is complete, the data will be either deleted or returned to the customer as requested.

How data is collected

Rooks Move's contracts or agreements with its customers confer that those customers have a legitimate reason to provide any such data and that Rooks Move can store and process such data on their behalf. Rooks Move only obtains data either directly from contracted customers (this includes other third parties working with the customer) normally via email or personal written recording and is stored electronically using PCs and Cloud based system, such as Microsoft® Office 365. Sometimes data is recorded in traditional note form and all reasonable steps are taken to secure this data when this is required, usually by transcribing into electronic form and stored in the same systems. Any Personal or High Security Data is then redacted.

Third Party email addresses are only collected by default and retained as part of legitimate business activity. Details are normally retained in email body and only converted to directly held data (e.g. Outlook Contacts), when trading relationships between customers and third party require this and permission given by that Third Party to do so.

Rooks Move does not engage in email marketing to its customers. Rooks Move does not engage in speculative email marketing to prospective customers or use bought lists of prospects.

Rooks Move's website does not store data but does temporarily collect data from its Contact Forms that is then sent via email systems to Rooks Move email addresses and then handled in accordance with these policies.

How Data is Stored

Rooks Move computer systems are backed up to a Cloud-based system. Rooks Move uses Microsoft® One Drive or Office 365, recognised encrypted back-up services with zero password knowledge, which saves onto multiple EU based servers.

Rooks Move uses Cloud-based business accounting package FreeAgent™ to run its book-keeping and invoicing. This system does store personal data necessary for normal business activity (e.g. generation of invoices etc.) FreeAgent™ is responsible under GDPR for its own policies and therefore handling of data used by Rooks Move.

Rooks Move does not operate its own dedicated database system (e.g. SQL Server, MySQL) that holds or collects any data defined below, other than use of Cloud-based business accounting package FreeAgent™

By request of the customer, data may occasionally be mutually shared via files with customers using Dropbox. Rooks Move does store data in some of the categories defined below on Dropbox for archiving purposes, for example invoices required for retention by HMRC. Dropbox is not an encrypted system and zero password policy is not in force due to its operation design.

All Rooks Move Computers & Servers that hold data are encrypted using Microsoft® Windows Bitlocker™ and password protected. Laptops are enabled with BIOS passwords at start up.

Smartphones, USB and portable hard drive devices used for moving or accessing data are all encrypted. Two stage authentication is used on any data-accessing App along with an App Locker. Files nested under these apps are also password protected. Find my Phone services are also enabled to enable full data wipe in the event of Smartphone loss.

Definitions of Data Sensitivity

Highest Security

This includes data held to carry out Rooks Move's work for its customers and all data categorised as *sensitive* under the DPA. However, Rooks Move has no requirement to hold any data under the DPA *sensitive* definition of data. The following categories are not defined as *sensitive*, but are considered by Rooks Move as requiring higher security:

- Usernames and website logins
- passwords
- Computer or Device PINs or Passwords
- Access codes to remote software
- IP Addresses
- SSIDs and WPA codes

Personal Data

This includes any personal home addresses, email addresses or telephone numbers even if associated to a business, where that business is run from a Private Home Address or Sole Trading establishment.

Business Data

This includes any job titles, business addresses, business email addresses or telephone numbers. Any data containing a mix of business and personal data is classified as Personal Data.

Third Party Suppliers

Rooks Move uses third party suppliers who may have access to data controlled by Rooks Move. In each case, Rooks Move has seen or holds copies of their data protection policies and has a contract with them that includes a confidentiality and data protection clause. These Third Parties include:

- Microsoft®
- IntY
- Sophos
- Avast AVG
- FreeAgent™
- M247
- TeamViewer