Data Protection and Security Policy

Notice

We provide information to our Customers and to our overseas agents and staff members. We try to work with Agents with likeminded attitude to Data Security Management such as FIDI Agents.

Choice and Consent

By accepting our quotation, due to the nature of our industry, our customers are authorizing us to use sensitive data in order to carry out and complete the relocation. It is at the consent of the customer to provide additional information that may not strictly be required in the course of the relocation.

Collection

We will ask Customers to provide us with confidential information either through e-mail or by personal pick-up.

Use, Retention and Disposal of Data

Staff are trained on the importance of data confidentiality. Use of data, such as Passport Copy etc. is limited to the purposes of the removal only. All correspondence between staff member on any given file is entered into our move management system for greater transparency.

All job files must be retained for a period of 10 years. Information stored on the computer is protected and hard files will be shredded after that period. Soft files deleted.

Access

Each staff member has a log in username and pass code to enable access to their own computers. Other staff members will not be able to access their files. Email access to other staff members are handled through IT tickets with approved process from HR and direct supervisor.

Our in-house built Intrack system is equipped with functions to protect confidential data. Staff is trained by senior management to understand the importance of data management.

Disclosure to Third Parties

Disclosure to third parties will only be made where the agent or supplier acts as an agent to Move One with similar principles.

Security for privacy

In order to protect private data, only authorized staff are able to access the file in the computer system corresponding to an individual customer. Other employees will automatically be blocked from access to those files.

Individual coordinators handle specific corporate accounts and only they will have access to those files.

The authorized manager will be able to access all accounts. This way data protection is heightened and access to personal data is limited to only key staff members.

In an effort to become paper free, all communication is attached within the computer system. Therefore the person responsible for the file is able to upload any document and send it to the Corporate Account or private customer on demand.

Quality

Data is limited to each file in our systems, this also provides a system to ensure accurate, complete and relevant personal information is uploaded in the computer in each correct file to increase efficiency and security.

Monitoring and enforcement

We provide in house training to ensure proper use of our systems and also to make staff aware of the importance of Data Protection.

Complaints

Any complaint or escalation regarding data privacy would immediately be communicated by the Move Coordinator to his/her line Manager. For a serious matter the management would become involved and the case reported to the local authorities such as the Police Force.

Review Procedure

We review all aspects of our Quality Manual on an Annual Basis. There will also be individual meetings and training to ensure that the above procedure is being adhered to.