



Data Privacy & Protection Policy

In the normal course of business, **Orbit Ltd** in its quality of administrator of personal data, shall be required to collect various elements of **Personal Information** about our Customers and Partners, as required in order to perform the work on behalf our Customers and/or Partners.

Likewise, the company shall also be obliged to disclose some of this Personal Data to our Partners in order for them to perform work on our behalf for the benefit of our Customers.

GDPR implementation requires some changes and their effect on the business are:

- 1/ Territory coverage;
- 2/ Our duty to request Customer consent, when Data management is not effected under contract obligations or legal requirement;
- 3/ Private individual rights;
- 4/ Juvenile individual consent;
- 5/ The right to be “forgotten”;
- 6/ Data exchange;
- 7/ Duty to inform Competent Supervisory entity in case of breach of Data Privacy;
- 8/ Security in use of technical and organizational methods;
- 9/ Employment of Data Protection Officer - DPO in charge on Data Privacy;

Application aspects of GDPR-Data Privacy and Protection:

- 1/ Business processes
- 2/ Jurisdictional aspects
- 3/ IT systems
- 4/ Information Security
- 5/ Physical security
- 6/ Data Exchange

Purpose of Data Privacy & Protection Policy:

It is our aim to Collect only the information relevant for the performance of Job/Move/Transaction.

- Our Customers and Partners (subject to Data Privacy Protection) shall be duly and actively informed of this requirement for the requested information, what Data we will use in our systems, by what purpose and based on which requirement, to whom we present their Data as well as how they can use their rights.
- The Company shall give the Customer the opportunity to accept our request for the relevant information or decline
- However, if a Customer decline, then the Company shall not be able to perform the required work on their behalf.
- Unless we hear to the contrary from a Customer, we shall assume **Explicit Consent**.
- This information shall be kept Strictly Confidential and shall only be Collected, Used, Stored, Disclosed and Retained by those directly involved in and for the performance of the relevant work and by maintain strict rules of confidentiality.
- This Data shall be available for the Customer to review and update upon request.
- Thereafter, the said information shall be disposed of following the legally required Retention Period for such Data. Disposal shall be by way of an appropriately secure and approved method.
- In the event that an incident is identified, this should be reported, in the first instance, to the Data Protection Officer (DPO), who will investigate the matter.

Should it be found that the reported incident is in fact a breach of the above, DPO shall then escalate the matter to The CEO and The President of the company and supervisory entity will be notified within 72 hours.