

Data Privacy Protection Policy

Information is a major asset that Transpack has a responsibility and requirement to protect. Protecting information is not simply limited to covering the data (electronic data or paper records) that the Organisation maintains. It also addresses the people that use them and the processes they follow. This Data Protection Policy addresses all these areas to ensure that high confidentiality; quality and availability standards of information are maintained.

The following policy details the basic requirements and responsibilities for the proper management of data at Transpack. The policy specifies the means of information handling and transfer within the Business.

This Data Protection Policy applies to all the systems, people and business processes. This includes all Executives, Departments, third parties and agents of the Organisation who have access to the Clients' Information or information used by Transpack.

Types of Information:

Client Information (including personal details)
Financial Information
Operational information
Contractual Details (financial arrangements with the vendors.)

The information is collected through Pre move survey forms as well as from the agents via emails. This data is also made available on the documents transmitted for example on Airway Bills, Bill of Ladings, Pre advise and Waybills received from the agents.

Definition

This policy is applied whenever client's' information is used. Information can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically.
- Communications sent by post / courier or using electronic means.
- Speech.

Accountability:

- Packing department / operations department is accountable along with the management for maintaining the data privacy policy maintained.

Management:

- Data Processing Activities takes place during the opening of a file (Procedure for Contract Review), Billing a client for incoming and outgoing shipments, Customs Clearance of shipments, Pre move surveys, deliveries and warehousing.
- Data is documented that is collected from the client. The information is collected via premove survey form, an incoming email from an Origin Agent. Data is collected from the client directly in case of an outgoing shipment where Transpack is the booker. All the data received is stored electronically and saved to the common server with restricted access. This information is also kept as copies in the physical file. The information collected is shared with operational staff, customs authorities, transporters and insurance brokers if insurance is requested in case of outgoing shipments.
- Personal data collected from the clients includes name, address, nationality, origin address and/or destination address, visa details.

Notices for data protection policies:

- The notice of Transpack's Data Protection Privacy Policy is published in emails sent out to clients, agents, vendors (third parties).
- The notice is also mentioned as part of the terms and conditions in the quotations sent to the agent.
- Copies are also distributed to each department to ensure communication and adherence to the policy. (Distribution Lists)

Choice & Consent:

- All quotations has a clause in the "terms & conditions" part stating that any information collected shall only be used for official purposes and maybe shared, if needed, with third parties. These quotes are either shared directly with the client or the agent. Any unauthorized disclosure if prohibited.
- Consent is taken in the form of an email or a document signed.

Collection:

- Information is collected EITHER via a pre move survey form OR via an email received from the agent assigning Transpack a booked move or by requesting a survey. Information is also collected from Client in some cases.
- Some sensitive information is also taken by passport and/or visa for Pakistan. The visa here concerns the work permit or temporary work visa.

Use, Retention & Disposal of Information:

- Confidentiality notices on signatures in emails are used. Any personal information collected will only be used for intended purpose only, for example details to be given on Bill of Ladings and Airway Bills will require client names and addresses.
- All types of information will be retained and will not be shared with any one.
- Information collected is used only for relocation purposes, in order for deliveries to take place, in case of an export. The information is retained in a physical file as well as correspondence done for the job in process over emails. We close files at the completion of the job. Information on soft copies goes in to back ups.
- Retention period is for ten years, however, the information collected is used only up to the time a job is in process. Once the job is complete the file is physically closed and kept in storage for ten years.
- The files are disposed off either by shredding them or burning them in a controlled environment.

Access:

- Clients are given access for review of their information via email correspondence and quotations.
- Agents are given access to their client's information via WAYBILLS and/or Shipping Advice sent to them prior to export of a shipment. In case of imports, the quotations also gives details of the client received from the agent for review and/or updating.

Disclosure to Third Parties:

- The client information disclosure is only limited to the B/L or Airway bill presented to the custom's authorities at the time of clearance.
- They also check the passport physically for exit entry stamps.
- Our quotes mention the privacy protection statement as well for the agents.



Security for Privacy:

- All information relating to a client is logically put on the common server for sharing information. However, the admin grants editing privileges only to Operations and Packing Department. The finance department retrieves the relevant information from the physical file itself.
- Physically, all move files be kept in a lock with the International Division; sign off is required as written authorization from the international department to retrieve the file.
- Procedure to Handle Potential Data Breach is followed to avoid security breaches leading to loss or unauthorized access to the personal data.

Quality:

- We maintain all information collected in a file opened for the purpose of record keeping of all inters continental shipments.
- Any information shared on the emails remains with the staff personnel addressed to.

Monitoring & Enforcement:

Monitoring is an integral part of ensuring compliance and enforcement of all policies maintained at Transpack. The management representative is responsible for monitoring the privacy policies.

Simple steps include, but are not limited to:

Interactive training sessions are carried out where all the policies and procedures are reviewed with the staff. Auditing and reviewing of documentation in all departments is also carried out; (Procedure for Internal Quality Audits (MR/2/004)); frequency of these internal audits is twice a year. Reports are documented, any non-compliance is documented and follow-ups are also planned and discussed in the Management Review Meetings held quarterly.

Any escalation incidents are dealt with a stepwise methodology using the Procedure for Corrective & Preventive Action (MR/2/005), evaluating the risks, discussing the problem with the people involved. In order to avoid the recurrence of the dispute we shall review our policies, enhance trainings and review all the security protocols in place to maintain data privacy at Transpack.