www.packimpex.ch

tailoring relocation solutions

packimpex.

Data Security Policy

25 August 2016

Data Security Policy

Purpose, scope and validity
Being discreet and ensuring the customer's confidentiality are essential components of our professional ethics. The purpose of this policy is to ensure that all Packimpex staff, external partners and subcontractors are clear about the purpose and principles of Data Protection and to ensure guidelines and procedures in place are consistently followed.

This Data Protection Policy is applicable to all employees of Packimpex as well as any third party company or person performing work for or on behalf of Packimpex (hereafter referred to as "Employees" and "Partners").

Implicit consent
Any customer ordering services from Packimpex will be notified of this data security policy and consent with its conditions is implicitly given. Should customers not agree, partially or entirely, with the content of the policy, Packimpex needs to be notified in writing before service delivery has started. Packimpex reserves the right to cancel services in this case if personal data is required to fulfill

Any partner accepting work from Packimpex will also be notified of this data security policy and implicitly agree with the policy and guarantee its application.

Definition of personal and confidential information
Personal information is defined as information that is not publicly available and cannot be acquired without any reservations.

The typical personal information we collect on individuals would usually include (but is not limited to)

- Name
- Address
- E-mail address
- Contact details
- Identification numbers (such as social security number or similar)

In addition to the above mentioned personal information, confidential information may be collected and may include

- work contracts
- lease contracts
- income related information

Information collected on employees of Packimpex or its partners is also considered as personal information and the same regulations apply analogously.

Personal and confidential information or data may be collected through online forms, move surveys, phone calls, emails, social networks, or any form of communication that includes the collection of information with the explicit or deduced consent of the client.

Quality of data, access to data, modification and disposal

Packimpex and partners will store personal data for as long as needed to fulfill the stated purposes or as long as required by laws and regulations. For Switzerland, the current duration of storage of personal data is 10 years. Past this date, Packimpex and partners will appropriately dispose of such information.

Customers may request at any time to obtain access to personal data that Packimpex or Partners hold on them and to verify its accuracy and request update and modification. This request has to be addressed to dataprivacy@packimpex.ch. It is not possible to request disposal of personal information once service delivery has started and for as long as legal obligations to retain data apply.

Should the requested information be incomplete, the applicant must notify Packimepx within five working days and request the correction of the error. Should Packimpex need any additional information from the applicant, this must be provided within two months of the request. If the customer does not provide the information, the process will be regarded as completed.

Confidentiality, Secrecy Requirement, Professional Secrecy

Personal data and other confidential information is collected relating to the provision of relocation services. Personal information received from customers both private and corporate will be used solely for the purpose of delivering our approved services. Packimpex and its expatriate community partner Hello Switzerland are permitted to use personal data in order to address relevant and value adding information on Switzerland and its particularities for newcomers to this country unless otherwise specified by the customer by e-mail to dataprivacy@packimpex.ch. The use of confidential information for marketing purpouses is not permitted.

Employees and partners are not allowed to disclose confidential or personal information to third parties or otherwise exploit confidential information. For employees this restriction is valid for their time of employment as well as after their employment has ended. This obligation to secrecy also applies to the company's internal information, documentation and resources.

Employees and partners agree to keep confidential and not to disclose, directly or indirectly, any information regarding Packimpex's business, including without limitation, information with respect to operations, procedures, methods, accounting, technical data or existing or potential customers, or any other information which Packimpex has designated as confidential.

Employees and partners shall not, either during the term of their employment/service delivery or at any time thereafter, disclose any proprietary, secret or confidential information

of the company to any third party whatsoever. Employees leaving Packimpex will be required to return all records, in any format, containing confidential information.

Within Packimpex the obligation to secrecy applies furthermore to coworkers whose job does not require access to a customer's or coworker's confidential information.

Protecting information

Employees and partners shall secure all documents, work in process, training or other items incorporating any confidential or proprietary information in locked file drawers or areas to which access is restricted in order to prevent its unauthorised disclosure.

The same regulations apply, if work is conducted offsite or from home. Employees and partners shall secure all information taken off-site and prevent its unauthorized disclosure. Using such information in public locations such as Restaurants, train stations etc. is strictly prohibited.

Any document, work in process, training or other items incorporating any confidential or proprietary information taken home have to be returned to company premises immediately after usage.

Employees and partners are expressly forbidden to store or transfer confidential information on a non-authorized i.e. noncompany issued portable device (e.g. USB stick, laptop etc).

Access to company premises

Access to company premises is restricted to employees. Access for business partners and third parties can be granted during business hours and only when accompanied by company employees.

All company premises are key-locked outside business hours. Keys are handed out to employees on a needs basis and key-handover logs are maintained.

IT Infrastructure

IT infrastructure must be protected in the company's and the employee's interest and is a key element in securing data privacy. Packimpex-specific IT Infrastructure regulations are described in more detail in Annex I.

Partners confirm that they have implemented adequate IT protection measures within their companies.

Reporting of non compliances

Any non-compliance with the prescriptions of this policy needs to be reported within 2 days of its discovery to dataprivacy@packimpex.ch or any Packimpex employee (who will then forward it appropriately). All breaches will then be reported to and treated under the responsibility of a senior management member. An acknowledgement and possibly a first feedback shall be provided to the reporter within one week of the report of an incident.

Adherence to policy and consequences of non-compliance

Adherence to these regulations regarding the usage of electronic systems can be monitored. An abuse is considered to have occurred if the provisions of these regulations have not been followed or if employees breach their work duties. If despite all precautions, repeated or heavy offences against these regulations are discovered, the company may order a personal evaluation after issuing a warning and is entitled to seek compensation for any loss or damage.

An abuse is considered to have occurred if the provisions of these regulations have not been followed or if partners breach their duties during service delivery or any time thereafter. If despite all precautions, repeated or heavy offences against these regulations are discovered, Packimpex may terminate the relationship with a partner and is entitled to seek compensation for any loss or damage.

The company reports criminal offences in connection with child pornography, racism, etc.

The Employees and partners are fully responsible for the security and the adherence to these guidelines when using any physical information, work stations or communication devices.

Ownership, communication and review of policy

This data security policy is under direct ownership of the Executive Management Team at Packimpex and is subject to an annual review process.

The policy will be communicated to key stakeholders by various means and under the responsibility of the Executive Management team. In particular, the following stakeholders need to be notified:

- Employees
- Partner companies and other third companies within the supply chain
- Corporate customers
- Private customers

Annex I - IT Infrastructure of Packimpex

IT infrastructure must be protected in the company's and the employee's interest.

The use of the company's infrastructure for private purposes must be held to a minimum and must not impair the obligation to work. The obligation to adhere to the company's confidentiality interests also applies when using the infrastructure for business purposes, in particular in connection with the storage of business data. Usage of the infrastructure should not leave negative trails which may lead to the company. Irregularities must be reported to IT immediately.

The employee acknowledges that the use of communication may be recorded for technical purposes.

Computer work station and laptop

The selection, acquisition and installation of PCs, electronic agendas, peripheral devices and software are the sole responsibility of the authorized IT person or his delegate. It is prohibited to install or to download programs from the internet. The connection of external PCs to the company's network is not permitted. The "C" drive is exclusively reserved for system files and programs and can be accessed, over-written or even deleted by IT at any time. Access to the technical resources is provided through a personal password. It is forbidden to share passwords or to maintain departmental password lists.

A business PC may be used only by designated company employees; it is forbidden for another person to use such PCs. Should the employee resign or if the equipment is not being used, the equipment including all accessories must be returned to the supervisor immediately.

Is an employee leaving the company his/her user accounts within the Packimpex environment, are deactivated immediately. The line manager has to ensure that the IT is informed about any leaving employee.

Virus protection

No e-mails shall be opened which have been received from suspicious parties and/or with a suspicious subject. Attachments of unknown source shall not be saved to the companies' media. Special caution is required with data storage devices such as USB sticks, discs, CDs, ZIP drives, etc. since these storage devices may contain viruses as well. Antivirus Software is Installed and maintained by the IT department.

Backup

IT staff ensures that all Confidential Information is backed up daily to disk. Weekly and Monthly Backup are stored to Tape. Monthly Backups are overwrite protected for one Year. One Backup every year gets archived and will be stored for 10 Years in line with Swiss legal requirements. All Backups are encrypted and regularly stored in a safe place outside of company premises.

The Backup Infrastruture is located in a different room from the Rest of the IT Infrastructure. This room has to be locked by IT staff at any time. Access to Backup Infrastructure by unauthorized staff is prohibited.

Server Infrastructure

Physical Access to Server Infrastructure containing confidential information is only allowed by authorized IT staff. These rooms have to be locked by authorized IT staff at all times. IT Staff has to ensure that all User Passwords granting access to confidential data are changed every 30 days. IT Staff has to ensure that all Admin Passwords are changed yearly.