www.packimpex.ch

tailoring relocation solutions

packimpex.

Data Security Policy

18 August 2020

Data Security Policy

Document Classification:	Public
Document Ref.	ISMS-DOC-A18-5
Version:	3
Dated:	18 August 2020
Document Author:	Damian Aebischer
Document Owner:	Damian Aebischer

Revision History

Version	Date	Revision Author	Summary of Changes
1	04.06.2018	Damian Aebischer	
2	15.07.2019	Eric Szilassy	Layout formatting
3	18.08.2020	Eric Szilassy	Change of the dataprivacy email address

Distribution

Name
Public

Approval

Name	Position	Signature	Date
Damian Aebischer	CEO	DA	15.07.2019
Damian Aebischer	CEO	DA	18.08.2020

Contents

1 Scope of Application

This document describes our company policies regarding the processing (use, protection, securing and storing) of personal information and data related to the services we provide to our private and corporate customers and the rights of our customers, suppliers, prospects and employees with regard to the data protection laws as set out in the General Data Protection Regulation (GDPR) and other applicable data protection legislation.

This document describes the obligations we have toward our customers, prospects and suppliers with regard to the lawful use of their data as set out in Swiss law and GDPR.

Packimpex is committed to protecting the confidentiality, transparency, integrity, availability and security of personal information and data which existing or potential customers, suppliers and personnel entrust us with. Our Privacy Policy includes norms and procedures concerning the use and the disclosure of the information of existing or potential customers, suppliers and our employees. Our Privacy Policy includes all procedures about the collection, storing, using, circulating, sharing and deleting of the personal data of our customers, suppliers and employees.

Our Privacy Policy includes protocols to meet all data subjects' rights:

- Right to access the data we hold
- Right to rectify the data if inaccurate
- Right to transfer the data (data portability)
- Right to (temporarily) stop the processing of data
- Right to withdraw the consent to process data
- Right to be forgotten
- Right to file complaint with the Privacy Authority

This Data Protection and Privacy Policy is a part of the overall privacy and security efforts of Packimpex. Other policies and control mechanisms also apply. The Privacy Policy applicable to our employees is provided in the employee handbook. The updates for all employees will be made available through the Intranet. The Privacy Policy for our prospects, customers and suppliers is available on the Packimpex website. Any changes to these policies are communicated as soon as possible to all involved via the intranet site (employees) and websites (customers, prospects and suppliers).

At all times, Packimpex relies on its employees, consultants, business partners and suppliers to properly follow up, develop, maintain, and operate our systems, databases, networks, and processes which keep personal data and especially sensitive data and information secure and properly used. This means that every person handling information and personal data has the responsibility to keep the information and personal data secure, no matter where the information and personal data is located: it applies to all computing systems, networks, databases, mobile devices, software, documents, paper copies, business processes, oral and any other transmission of information and personal data.

Penalties for violating these policies may include disciplinary actions up to termination of employment, or termination of the business relationship with our company.

2 Data Protection

To comply with GDPR and other applicable national and international data protection regulations, Packimpex informs its prospects, customers and suppliers how their personal data is protected through means of a Data Privacy Policy (on the website and along with quotations). This Privacy Policy states that Packimpex will ensure all rights under GDPR are adhered to, and that it will not share personal data with third parties outside the supply chain responsible for delivering the authorized services, or unless necessary to comply with the local and international laws and regulations. In the event that we need to share the personal data, data subjects will be informed as such in advance.

This Data Privacy 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”).

3 Definition of Personal Information

Personal data is any data that is related or can be connected to one (or several) identified or identifiable natural person(s). Personal data collected by Packimpex to provide the requested services include some of the below (but not exclusively):

- our customer’s names
- telephone numbers
- position
- address
- personal and business contact information
- personal documents such as (copies of) passports, (copies of) identity cards
- visas and work permits
- financial information
- religious information
- educational information

All information and data collected and provided will be used by, retained by and disclosed confidentially to our supply chain or service providers selected by our customers on a strictly need-to-know basis, with the application of strict access rules.

4 Collection of Data

Personal data may be collected through online forms, phone calls, emails, social networks and promotional activities.

Furthermore, we monitor activities and register user activities with the use of cookies, social media plugins, and tracking tools on our website and social networks such as Facebook, Twitter, LinkedIn, and Google+.

5 Processing of Personal Data

Packimpex has a documented IT security policy. This policy contains all measures taken to guarantee security on all levels of processing information and personal data: legal, organisational, technical and physical measurements which we have in place. These measures are regularly reviewed and, if necessary, updated and communicated to all parties involved.

In short: all personal data is stored on secured databases and is protected by different means from unauthorised access. We work with personal passwords (see password policy) and a firm deletion policy (see deletion policy).

6 Purpose of Processing

Personal information received from both private and corporate customers will be used solely for the purpose of delivering the 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 about Switzerland and its particularities to newcomers to this country unless otherwise specified by the customer by e-mail to dataprivacy@packimpex.com. This implies that all personal data processed is merely based upon the legitimate grounds as provided by the applicable data protection legislations and more specific GDPR.

Data may also be used for direct marketing purpose to position information about our organisation, services and products in the form of newsletters. At the end of every newsletter, an unsubscribe option is offered and, if chosen, all corresponding personal data will be deleted.

7 Transfer of Data

Personal data will primarily be disclosed and provided to parties within the supply chain of Packimpex. Our service providers and business partners will receive data on a need-to-know basis, to fulfil their contractual obligations. All selected service providers will be obliged to sign a Data Protection Agreement (DPA). Any provider not completing the DPA will be removed from the supply chain.

The nature of our services requires us to disclose and provide data to third parties that are not part of our supply chain and who establish a direct contractual relationship with our customers. Such third parties are namely (listing not complete):

- Landlords and real estate companies
- Banks and insurance companies
- Telecommunication companies

This submission is always linked to provision of services as outlined in our mandate agreements. Furthermore, we use data collected on website and social media usage to analyse and monitor effectiveness of marketing and social media campaigns and to define pseudonymised user profiles.

In addition, we will share your information with third parties if this is required to provide the services you request and/or to analyse your user activity. If this is necessary for the purposes stated above, the disclosure may also be made abroad. Where our documentation or website contain links to third party websites, after clicking on these links, Packimpex will no longer have any influence on the collection, processing, storage or use of personal data by third parties and assumes no responsibility for it. Personal data will never be sold to any party.

OUR POLICIES AND PROTOCOLS:

8 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 off site or from home. Employees and partners shall secure all information taken off site and prevent its unauthorised 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 has to be returned to company premises immediately after usage.
Employees and partners are expressly forbidden to store or transfer confidential information to a non-authorised i.e. non-company-issued portable device (e.g. USB stick, laptop etc).

When the employee working with the personal data of a customer, prospect, business partner, supplier or other employee gets up, leaves their desk or goes home, they must lock their computer screen or turn the power off. In all cases, our IT specialists have ensured that company systems and screens lock automatically after 15 minutes if no activity is registered.

9 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 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.

10 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.

11 Declaration of privacy at the bottom of e-mails

All e-mails sent by Packimpex employees include an automatic footnote/disclaimer which states that any information included in the e-mail contains privileged and confidential information and that if the recipient received an e-mail in error, Packimpex should be notified and the e-mail deleted. (Even if the e-mail does not contain such information, the note should be included as a contingency.)

12 Confidentiality clauses and DPA

All employees sign a confidentiality clause regarding the handling of personal data. This confidentiality clause is set out in the employee handbook which is an integral part of employees' work contract.
All consultants and business partners working for Packimpex must sign a Data Protection Addendum/Agreement (DPA) that obliges them to meet all requirements under the applicable data protection legislation and prohibits them from disclosing any personal data about Packimpex customers and/or employees. At all times, they must comply fully. If any irregularities are discovered, this might (depending on the gravity) lead to the termination of the relationship with Packimpex. The consultants and business partners shall have limited access to the databases on a strictly need-to-know basis when the information is needed to perform their services.

Employees and partners are not allowed to disclose confidential or personal information to third parties except for the purposes stated above. 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 co-workers whose job does not require access to a customer's or co-worker's confidential information.

13 Procedure to ask for the change, update, correction, deletion or transfer of personal data

Every natural (identified and identifiable) person has the right to ask for access to their data, ask to update/correct the data when not correct/accurate or ask to delete their personal data (right to be forgotten), and ask to transfer their data to another provider.

Customers are entitled to:

- Verify the information that Packimpex holds on them – for free
- Request to have the personal data changed, updated, deleted or transferred (in conformity with the data protection regulation)
- Request the information (via the telephone) or in writing
- In all cases, prior verification of the identification of the customer/applicant is required.

Request by telephone (to exercise the above-mentioned rights)

- The request to exercise any of the above-mentioned rights with regard to their personal data will only be granted once the identity of the person is verified and validated. Whenever we

receive such a request, we must ask the person to confirm their request in writing. This written request must be forwarded to our helpdesk immediately.

Request in writing (to exercise the above-mentioned rights)

- The request to view the personal data request must be forwarded to our helpdesk immediately.

Under no circumstances is an employee allowed to undertake any action themselves except to immediately forward the request to the helpdesk.

The following natural persons can exercise above-mentioned rights of modification of personal data:

a) The customer, provider, supplier, consultant, business partner or intermediary (everyone acting in their name)
b) An authorised and mandated representative

14 Data Breach Protocol

We consider any incident of incidentally misusing or revealing personal data, without any prior authorisation and which jeopardises the availability, integrity and confidentiality of the information or data and thus creates a risk for the data subject (customer, provider, supplier, consultants, business partner and intermediary), as a breach that should be registered in our data breach register.

For example:

- An employee who accesses the personal data of a customer outside of the limits of his work.
- The loss or theft of a work computer/laptop/mobile phone/paper documents that contain unencrypted personal data of a customer.
- Personal data sent to the wrong address, fax or e-mail because of an error.
- A customer informed you that they found their personal data online or any other inappropriate location.

Any potential breach of data needs to be reported to the helpdesk and such immediately, with a maximum of 12 hours after the discovery of the breach. The reporting is done via e-mail to dataprivacy@packimpex.com or telephone call to our IT support desk (+41 58 356 14 88).

If the breach was the result of the loss or theft of a computer/laptop/mobile phone, the IT department needs to be informed as well so that they can, together with the data breach team, take appropriate measures.

15 Data retention and deletion

Packimpex will keep the information and personal data stored for the duration of the provision of the services and as required by laws and regulations. After the mandatory period of storage has expired, Packimpex will dispose of the files as required per law or set out in the Privacy Policy.

16 Training of personnel

Packimpex will train its personnel at least once a year with regard to the content of this document to ensure the security, confidentiality, truthfulness and integrity of the personal data and information of its customers, providers, suppliers, business partners, consultants and employees. Every training session will be documented, including a list of the participants and the discussed topics. Throughout the year, all related questions anyone should have must be addressed to dataprivacy@packimpex.com.

17 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 party companies within the supply chain
- Corporate customers
- Private customers

The policy will be updated when necessary and without prior notice. Customers, suppliers, consultants, business partners and employees will be notified in writing.

18 Annex I - IT Infrastructure of Packimpex

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

The use of the company's infrastructure for private purposes must be kept 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 back to the company. Irregularities must be reported to IT immediately.

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

18.1 Computer work station and laptop

The selection, acquisition and installation of PCs, electronic agendas, peripheral devices and software are the sole responsibility of the authorised IT person or their 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.

When an employee is leaving the company, their user accounts within the Packimpex environment will be deactivated immediately. The line manager has the responsibility to ensure that IT is notified about any leaving employee.

18.2 Password policy

Passwords are strictly personal and never to be passed on to a colleague, except upon explicit approval of the IT and HR departments.

18.3 Virus protection

No e-mails shall be opened which have been received from suspicious parties and/or with a suspicious subject. Attachments from an unknown source shall not be saved to the company's 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. Anti-virus software is installed and maintained by the IT department.

18.4 Server infrastructure and backup

Packimpex does not run its own IT infrastructure. All servers are managed and operated by an external provider with appropriate qualifications. Packimpex IT ensures service level agreements are in place that regulate all relevant topics such as (but not limited to) physical access to server infrastructure, encryption of data, password policies and backups.
Backups are ensured by the service provider on a daily basis. Backups are encrypted and stored in physically separated locations.