Eurasia FCI Transportation Service Co., Ltd.

RELOCATIONS BUSINESS

DATA (PRIVACY) PROTECTION POLICY

EDITION H

Feb. 2023

Year	Revision	Prepared by:	Reviewed by:	Approved by:
2019 Aug	EDITION E	Elaine Wang	Elaine Wang	Kevin Chuang
2020 Aug	EDITION F	Elaine Wang	Elaine Wang	Kevin Chuang
2021 Dec	EDITION G	Elaine Wang	Elaine Wang	Kevin Chuang
2023 Feb	EDITION H	Elaine Wang	Elaine Wang	Kevin Chuang

TABLE OF CONTENT

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 Eurasia FCI 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 Eurasia FCI as well as any third party company or person performing work for or on behalf of Eurasia FCI (hereinafter referred to as "Employees" and "Partners")..

Management of the Policy

Editing, review, approval

The editing and updating of the present policy are the responsibility of FCI Relocation Department.
The review and approval of the different editions of the policy is ensured by Management of FCI Relocation.

Issuing

The release is made by FCI relocation department manager, under the authorization of the general manager.

Reviews

A review must be made at least once a year.
A review meeting should be arranged which should review all elements as described above and evaluate if these are still accurate. The review meeting shall be attended by relocation department manager, relocation sales manager, customer service supervisor and operation supervisor.
Normally, this review meeting shall be arranged in August of each year by relocation department manager. In case the elements should be updated the policy should be updated with the new and improved contents and be implemented and communicated to all staff.

Implicit or Explicit Consent

Any customer ordering services from Eurasia FCI will be notified of this data security policy and consent with its conditions is implicitly given. Privacy is important to everyone. It is the nature of our business that we need to collect, process, use and retain non-public personal information. It is important to us that our customers, employees and other individuals with whom we work can trust us in taking care of their non-public information. We are committed to respecting those individuals whose personal information we handle in operating our business and delivering our services in accordance with applicable law, our own policies and those of the professional standards to which we are certified.

Should customers not agree, partially or entirely, with the content of the policy, Eurasia FCI needs to be notified in writing before service delivery has started. Eurasia FCI reserves the right to cancel services in this case if personal data is required to fulfill
Any partner accepting work from Eurasia FCI 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
- Home Address
- E-mail address
- Contact details
- Identification numbers (such as social security number or similar)
- Date of Birth

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

- Work contracts
- Lease contracts
- Financial or income related information
- Physical characteristics
- Information of Medical or health conditions
- Racial or ethnic origin
- Political opinions
- Religious or Philosophical beliefs
- Trade union Membership

- Sexual Preference
- Information related to offenses or criminal convictions

Information collected on employees of Eurasia FCI 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.

CORPORATE RESPONSIBILITY

- Quality of data, access to data, modification and disposal

Eurasia FCI 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. In China, the current duration of storage of personal data is 10 years. Past this date, Eurasia FCI and partners will appropriately dispose of such information.
Customers may request at any time to obtain access to personal data that Eurasia FCI or Partners hold on them and to verify its accuracy and request update and modification. This request has to be addressed to relocations@shanghai.eurasia.com.cn. 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 Eurasia FCI within five working days and request the correction of the error. Should Eurasia FCI need any additional information from the applicant, this must be provided within two months of the request. If the applicant does not provide the information, the process will be regarded as completed.
Destroy/Disposal:The document is smashed through shredder and privacy data in computer disposal is through authorized professional service vendor and managed by Eurasia FCI recor ds management Dept.

Supply Chain

- 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 purposes of delivering our approved services. The use of confidential information for marketing purposes is not permitted. Employees, service providers 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, service providers and partners agree to keep confidential and not to disclose, directly or indirectly, any information regarding Eurasia FCI'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 Eurasia FCI has designated as confidential.
Employees, service providers 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 Eurasia FCI will be required to return all records, in any format, containing confidential information.
Within Eurasia FCI 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, service providers 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, service providers 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, service providers 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. Eurasia FCI-specific IT Infrastructure regulations are

described in more details_网络和系统安全管理规定\访问控制管理规定\数据备份管理规定
Partners confirm that they have implemented adequate IT protection measures within their companies.

Security for Privacy

Eurasia operate a strict Data (Privacy) Protection Policy which sets out our commitment and instructions for maintaining and protecting the information we hold in compliance with the FIDI FAIM Privacy Principles, including:

- How people interact with us, either online or throughout the course of our services. Data collected is fairly and lawfully processed.
- We collect, process, store and disclose information only for the purpose intended and always according to a legal basis of processing, either with your consent, as part of a contractual agreement, due to a legitimate business interest or through our legal obligations regarding compliance. Data held is adequate, relevant and not excessive.
- We ensure non-public data is protected by appropriate security procedures with significant access controls to safeguard from loss, damage or unauthorized access at all times and is only processed in line with your rights.
- We do not keep information for longer than necessary in order to fulfil required services and comply with legal regulations. We ensure that after this date information is securely disposed of or deleted.
- We strive to ensure the data we hold is accurate and up to date and provide reasonable access to individuals to view and update their information, where necessary.
- Data is not transferred to other countries without adequate protection
- Eurasia FCI is committed to maintaining and protecting the information it holds on its customers and its operations. This includes protection from theft, loss or corruption through external or internal sources and contingency planning in the event of systems failure.
- Eurasia FCI is committed to a policy of protecting the rights and freedoms of individuals with respect to the collection, processing and storage of their personal data (by electronic and/or paper means) and complies with The Data (Privacy) Protection Policy.
- All employees, partners, subcontractors and suppliers are responsible for ensuring that we protect the rights and freedoms of individuals in compliance with data protection laws.
- Employees, partners, subcontractors and suppliers should familiarize themselves with the Data Security and Information Assurance policy and their obligations under it, any non-compliance will be treated seriously and may involve disciplinary action.

When we receive a complaint from a person we make up a file containing the details of the complaint. This normally contains the identity of the complainant and any other individuals involved in the complaint.

We will only use the personal information we collect to process the complaint and to check on the level of service we provide. We do compile and publish statistics showing information like the number of complaints we receive, but not in a form which identifies anyone.
We usually have to disclose the complainant's identity to whoever the complaint is about. This is inevitable where, for example, the accuracy of a person's record is in dispute. If a complainant doesn't want information identifying him or her to be disclosed, we will try to respect that. However, it may not be possible to handle a complaint on an anonymous basis. Similarly, where enquiries are submitted to us we will only use the information supplied to us to deal with the enquiry and any subsequent issues and to check on the level of service we provide.

In many circumstances we will not disclose personal data without consent. However, when we investigate a complaint, for example, we will need to share personal information with the organization concerned and with other relevant bodies. Further information is available in our Data (Privacy) Protection Policy about the factors we shall consider when deciding whether information should be disclosed.

You can also get further information on:

- Agreements we have with other organizations for sharing information;
- Circumstances where we can pass on personal data without consent for example, to prevent and detect crime and to produce anonymized statistics;
- Our instructions to staff on how to collect, use and delete personal data;

How we check that the information we hold is accurate and up to date.

Monitoring and Enforcement & Reporting of Non-compliance

We monitor compliance with this procedure and our privacy notice. All parties responsible for compliance are aware that any breach may lead to action being taken against them.
Risk assessments will be undertaken and recorded by the Finance and IT Director in consultation with IT providers.
Action required to remove, or control risks will be approved and actioned the Finance and IT Director in consultation with IT providers.
This procedure and related policies will be reviewed regularly in light of any legislative or other relevant developments.
If you believe your information is not handled in accordance with the applicable law or our privacy policies you may submit a complaint to our Quality & Compliance Department. You can email to relocations@shanghai.eurasia.com.cn or any Eurasia FCI 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, Eurasia FCI may terminate the relationship with a partner/employee 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 protection policy is under direct ownership of the Executive Management Team at Eurasia FCI 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