Privacy Policy and Data Protection Management

JK Moving and its affiliated United States subsides (hereinafter collectively referred to as "the Company", "we", "us" or "our) adhere to the Privacy Shield Framework concerning the transfer of personal data from the European Union ("EU") and Switzerland to the United States of America. According, we follow the Privacy Shield Framework published by the U.S. Department of Commerce (the "Principles") with respect to all such data. If there is any conflict between the policies in this privacy policy and the Principles, the Principles shall govern. The U.S. Federal Trade Commission has jurisdiction over the Company compliance with the Principles. This privacy policy outlines our general policy and practices for implementing the Principles, including the types of information we gather, how we use it and the notice and choice affected individuals have regarding our use of and their ability to correct that information. This privacy policy applies to all personal information received by the Company whether in electronic, paper or verbal format.

Definitions

"Personal Information" or "Information" means information that (1) is transferred from the EU and Switzerland to the United States or is collected from the individual customer; (2) is recorded in any form; (3) is about, or pertains to a specific individual; and (4) can be linked to that individual. "Sensitive Personal Information" means personal information that reveals race, ethnic origin, and sexual orientation, political opinions, religious or philosophical beliefs, trade union membership or that concern's an individual's health.

Principles

Management – The Company collects data or personal information that is relevant to the move. All data is stored securely on our servers and viewed only by members of our staff who have had background checks and drug screenings conducted. Employees must take all necessary steps to prevent unauthorized access to identifiable individual information, protected health information, company private corporate strategies, competitor sensitive information, trade secrets, specifications, customer lists, personal information, credit card numbers, and research data. All hosts used by the employee that are connected to the JK Internet/Intranet/Extranet, whether owned by the employee or JK, will be continually executing approved security software that is update automatically as new threats are identified. Any breach/loss or potential breach/loss of a shipment, information pertaining to a shipment, or included in shipment must be reported to an operational supervisor immediately.

Notice – Company shall inform an individual of the purpose for which it collects and uses the Personal Information and the types of non-agent third parties to which the Company discloses or may disclose that Information. Company shall provide the individual with the choice and means for limiting the use and disclosure of their Personal Information. Notice will be provided in clear and conspicuous language when individuals are first asked to provide Personal Information to the Company, or as soon

as practicable thereafter, and in any event before the Company uses or discloses the Information for a purpose other than for which it was originally collected.

Choice – The Company will offer individuals the opportunity to choose (opt out) whether their Personal Information is (1) to be disclosed to a third party or (2) to be used for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual. For Sensitive Personal Information, the Company will give individuals the opportunity to affirmatively or explicitly (opt out) consent to the disclosure of the information for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual. Company shall treat Sensitive Personal Information received from an individual the same as the individual would treat and identify it as Sensitive Personal Information.

Collection – Personal Information collected from a customer will only be collected if pertinent to the service provided. The Company will never ask for personal information that is not necessary in order to facilitate a move.

Use, Retention and Disposal – Our data is used solely for the reasons given in our notice. Personal information will remain stored in our secure servers until the Company no longer has reason to store it.

Access to Individuals (Private Customer or Corporate Accounts) – If requested, individuals will be granted access to their personal information stored on our servers.

Quality - All personal information gathered by the Company will be verified with the individual before it is inputted into our system.

Monitoring and Enforcement – The Company monitors the use of personal information, in the case that there is evidence indicating improper use of personal information all employees are required to notify their supervisor. The Company maintains 24 hours monitoring of our information systems and facilities and will be alerted immediately upon detection of any issues that prevents optimal service. Upon detection, the Company will make use of the established escalation and call tree, which begins with a Senior System Administrator and then escalated to the Director of IT before briefing the Chief Information Officer after 3 and 6 hours, respectively.

Onward Transfers – Prior to disclosing Personal Information to a third party, Company shall notify the individual of such disclosure and allow the individual the choice (opt out) of such disclosure. Company shall ensure that any third party for which Personal Information may be disclosed subscribes to the Principles or are subject to law providing the same level of privacy protection as is required by the Principles and agree in writing to provide an adequate level of privacy protection. Company is liable for onward transfers to third parties and will comply with the Notice and Choice Principles before transferring Personal Data to a Third Party who is not an agent of Company.

Access Requests by Public Authorities – Company may be required to disclose your personal information in response to lawful requests from public authorities, including to meet national security

or law enforcement requirements. Where permitted by law, the Company has the option to issue reports relating to data privacy inquiries.

Data Security – Company shall take reasonable steps to protect the Information from loss, misuse and unauthorized access, disclosure, alteration and destruction. Company has put in place appropriate physical, electronic and managerial procedures to safeguard and secure the Information from loss, misuse, unauthorized access or disclosure, alteration or destruction. Company cannot guarantee the security of Information on or transmitted via the Internet.

Data Integrity – Company shall only process Personal Information in a way that is compatible with and relevant for the purpose for which it was collected or authorized by the individual. To the extent necessary for those purposes, Company shall take reasonable steps to ensure that Personal Information is accurate, complete, current and reliable for its intended use.

Access – Company shall allow an individual access to their Personal Information and allow the individual to correct, amend or delete inaccurate information, except where the burden or expense of providing access would be disproportionate to the risks to the privacy of the individual in the case in question or where the rights of persons other than the individual would be violated.

Enforcement – Company uses a self-assessment approach to assure compliance with this privacy policy and periodically verifies that the policy is accurate, comprehensive for the information intended to be covered, prominently displayed, completely implemented and accessible and in conformity with the Principles. We encourage interested persons to raise any concerns using the contact information provided, and we will investigate and attempt to resolve any complaints and disputes regarding use and disclosure of Personal Information in accordance with the Principles. If a complaint or dispute cannot be resolved through our internal process, we agree to dispute resolution using (an independent resource mechanism) as a third-party resolution provider.

Amendments – This privacy policy may be amended from time to time consistent with the requirements of the Privacy Shield Framework.

Information Subject to Other Policies – The Company is committed to following the Principles for all Personal Information within the scope of the Privacy Shield Framework. However, certain information is subject to policies of the Company that may differ in some respects from the general policies set forth in this privacy policy. Under certain conditions, more fully described on the Privacy Shield website, individuals may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted.