Global Privacy Policy

https://www.aitworldwide.com/privacy-policy/

Global Privacy Policy

(Status: November 2026)

This Global Privacy Policy is designed to inform you about how AIT Worldwide Logistics ("AIT", "we", "us" or "our"), as Controller, collects, uses, and shares your personal data through our website (www.aitworldwide.com) (hereinafter, the "Site") and when you interact with us online or offline. .

By accessing our Site or using our services (hereinafter "Services"), you acknowledge that you have read and understand this Global Privacy Policy and that we will collect, use and disclose your data as set forth below.

Scope of Application

The present Global Privacy Policy is designed to apply to the visitors to our Site and users of our Services on a global basis and aims to provide you with a general overview of how we collect and process your personal data or information. The Global Privacy Policy is intended to comply with European standards under the General Data Protection Regulation (GDPR), however, the general information contained in this Global Privacy Policy shall also apply to visitors located or residing outside the European Union or European Economic Area.

Please note, that depending on your country, region, or state of residence, we are required to provide you with additional information relating to the processing of your personal data. This additional information is provided in the following Addenda:

- **Addendum A** - Additional Privacy Terms for Chinese Residents
- **Addendum B** – Additional Privacy Terms for residents of the United States of America
- **Addendum C** – U.S. Biometric Privacy Policy

Definitions

Personal Data / Personal Information: means any information relating to an identified or identifiable natural person ("data subject"). Personal data does not include de-identified, aggregated, or anonymized information that is maintained in a form that is not capable of being associated with or linked to you or a particular household or publicly available information from government records.

Processing: means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval,

consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Controller: means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

Data Processing Agreement: means an agreement concluded between a Controller and a Processor and regulates the use of personal data by the Processor.

Data Protection Officer: means the natural or legal person, appointed by a Controller or a Processor and responsible for ensuring, in an independent manner, that a Controller or Processor processes personal data in compliance with the applicable data protection laws.

EU-US Data Privacy Framework / UK Extension to the EU-US Data Privacy Framework / Swiss-US Data Privacy Framework: legal framework aiming at providing United States organizations with reliable mechanisms for personal data transfers to the United States from the European Union / European Economic Area, the United Kingdom, and Switzerland that are consistent with EU, UK, and Swiss data protection laws. Organizations participating in the EU-US Data Privacy Framework may receive personal data from the European Union / European Economic Area in reliance on the EU-US Data Privacy Framework effective July 10, 2023.

Processor: means a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the Controller.

Supervisory Authority: means an independent public authority responsible for monitoring the application of data privacy laws.

Contact Details of the Controller

As a general rule, we are the Controller of your personal data and our contact information is:

AIT Worldwide Logistics, Inc.
2 Pierce Place, Suite 2100
Itasca, Illinois 60143
United States of America
Email: dataprivacyoffice@aitworldwide.com
Phone: 1-800-669-4248

However, depending on the processing activity or the country you reside in, the entities appearing in following addendum may also act as Controller(s):

- **Addendum D** – List of Additional Controllers

Contact Details of the Data Protection Officer

We have appointed an external Data Protection Officer for AIT Worldwide Logistics group companies located in Europe. European residents can contact the Data Protection Officer under:

2B Advice GmbH
Joseph Schumpeter Allee 25
53 227 Bonn, Germany

E-Mail: aitworldwide@2b-advice.com

Non-European residents can contact the Privacy Team by email at dataprivacyoffice@aitworldwide.com.

Personal Data We Collect and Process, and the Applicable Purposes

1. Cookies & Tracking Technologies

To ensure our Site works properly and to provide the most up to date and relevant information, we use cookies and other technologies on our Site.

Cookies are small files or part of a file stored on an internet user's computer and which are subsequently read by a website server.

The types of cookies and other tracking technologies we use are:

Essential Cookies: essential cookies are necessary for our Site's functionality and cannot be disabled. We do not need to obtain your prior consent for the use of essential cookies. Processing data through essential cookies is based on our legitimate interest in ensuring the security and functionality of our Site.

Performance Cookies: performance cookies are used to enhance the performance and of our Site but are not essential to its use. However, without these cookies, certain functionality may become unavailable. You can manage your preferences for performance cookies on our site.

Analytics & Marketing Cookies: analytics and marketing cookies are used to determine user's / visitor's interests and to evaluate the effectiveness of our marketing campaigns or to provide better targeting for marketing purposes. You can manage your preferences for performance cookies on our site

For more information on the cookies and tracking technologies we use, and to manage your choices, please click on the Cookie icon at the bottom of the website of the left side.

2. Employment Recruitment

You have the possibility to apply to an open employment position. Open employment positions are available under www.aitworldwide.com/careers/job-portal/. We may collect the following categories of personal data during the employment recruitment process:

- Identification data;
- Contact details;
- Application data (e.g. Information Related to Candidate Qualifications, Past Employment, Interview Notes, References, Immigration Status & Documentation, Residency Permits & Visas);
- Demographic data (e.g. Date of Birth, Gender, Disability); and
- Financial data (e.g. banking details for reimbursement of travel expenses).

The collection and use of your personal data enables us to administer the recruiting process. Below is an overview of the processing activities and purposes as applicable to the employment recruiting process and the corresponding legal basis:

Processing Activity / Purposes	Legal basis
Creation / deletion of an applicant account in ICIMS	Your consent.
Creation of a job applicant file	Performance of a contract or pre-contractual measures.
Managing job applications	
Organizing interviews	
Assessing your skills, qualifications and interests in relation to the employment requirements of our company and your suitability for the specific job for which you are applying	
Arranging and / or reimbursement travel	
Communicating with you about the recruitment	Performance of a contract or pre-contractual

process and/or your application	measures or your consent
Communicating with you about possible future career opportunities	Your consent
Conducting background checks	Performance of a contract or pre-contractual measures and / or our legitimate interest
Compliance with applicable laws and regulations, or to protect the company´s legitimate interests (e.g., to defend AIT Worldwide Logistics against legal claims) in legal proceedings	Processing is necessary for compliance with a legal obligation or our legitimate interest

You provide us with most of your personal data. However, we may also obtain personal data about you during the course of the employment application process, as well as from third parties such as recruiting agencies.

Your personal data may be shared internally between our various departments or within the AIT Worldwide Logistics group of companies in the process of selecting candidates for employment with us.

Please note, that for the management of the recruitment processes, we use an applicant tracking system operated by iCIMS. iCIMS therefore acts as Processor and a Data Processing Agreement has been concluded. Please also note, that your personal data may be transferred to the United States. iCIMS has taken part to the EU-US Data Privacy Framework enabling the transfer of personal data from Europe to the United States.

We will retain your personal data for so long as necessary to carry out the purposes we have described above, or as otherwise required by applicable laws and regulations. As a general rule, if your application is unsuccessful, your personal data will be deleted according to the applicable local laws of the jurisdiction you reside in. If your application is successful, we will keep your personal data and delete it according to our Global Privacy Policy for Employees. Please also note, subject to legal retention obligations, the right to remove your application from iCIMS and to delete your account. If you have specific questions related to your application or our HR processes, please contact HR@aitworldwide.com or our Data Protection Officer. If you would like more information on how iCIMS processes your personal data, please visit their website: www.icims.com or contact their Data Protection Officer under privacy@icims.com.

3. Newsletter (AIT News Bulletins)

You have the possibility to subscribe to our Newsletter (https://www.aitworldwide.com/resources/news-bulletins/). Your personal data

(identification data and contact details) will exclusively be processed for providing you with updates and marketing emails via AIT News Bulletins. The legal basis for processing your personal data is your consent. Please note, that you can revoke your consent at any time in the future and unsubscribe from the newsletter by clicking the link in the footer of our emails. In that case, we will remove you from our recipient list.

Please note, that we use Mailchimp as our marketing platform. Mailchimp is considered a Processor and a Data Processing Agreement has been concluded. Please also note, that your personal data may be transferred to a third country, namely the United States. We have concluded Standard Contractual Clauses (Standard Contractual Clauses is a transfer instrument enabling the transfer of personal data from Europe to the United States) with Mailchimp to secure the transfer of personal data abroad. If you would like to get more information on how Mailchimp processes your personal data, please check their website: www.mailchimp.com.

4. Use of HubSpot

We use HubSpot, a Contact Relationship Management software, for our marketing activities (e.g. contact management and lead generation). The legal base for using HubSpot is our legitimate interest in optimizing and managing our marketing activities). The processing of your personal data (identification data, contact details, company data, content of the request, etc) is however based on your consent.

A Data Processing Agreement has been concluded with HubSpot Inc., who acts as Processor and recipient of your personal data. Please note, that your personal data may be may be transferred to and processed by HubSpot, Inc. in the United States and to other jurisdictions where HubSpot Affiliates and sub-processors have operations. HubSpot has taken part in the EU-US Data Privacy Framework enabling the transfer of personal data from Europe to the United States and has, where necessary, concluded Standard Contractual Clauses with its sub-processors to ensure a high level of security for the processed personal data. For more information, please visit the website www.legal.hubspot.com.

5. Contact

You have the possibility to contact us by using one of the forms available under https://www.aitworldwide.com/contact-us/ .

Depending on your request, we may collect and process the following categories of personal data:

- Identification data;
- Contact details;
- Company data / information; and
- Content of the request / enquiry.

The legal basis for processing your personal data is usually our legitimate interest in handling your request. If you are one of our customers, the legal basis for processing the information you provided to us would generally be the provision of Services.

In any case, your information will exclusively be processed for handling your request and will be shared with third parties only if required.

6. FasTrak My Shipment

You can use FasTrak (LINK) to track shipments / deliveries addressed to you. To track a delivery, you usually only need to enter a tracking number. We may require that you provide us with additional personal data (e.g. E-Mail Address, Mail Address, Phone Number) for services beyond tracking, for example to schedule a delivery. The data is processed for the purpose of fulfilling the shipment contract. We will keep your data for as long as necessary to fulfill our purposes, to execute our contracts, and to comply with any legal obligation. The retention period may differ per country based on applicable country laws.

7. My AIT

My AIT (LINK) is an online customer portal, which provides our customers with easy access to all their vital shipping information and activities, including quotes, claims, tracking, billing, etc. Access to My AIT is provided by the Sales Support department. To create an account in My AIT, customers are required to provide an e-mail address and to set up a password. The legal basis for the creation of an My AIT account is the consent of the customer. The personal data contained in My AIT will usually be stored until deletion of the account.

Please note, that it is not mandatory to file a claim or a complaint by creating an AIT account. You can also submit a claim or a complaint by contacting your contact person at AIT Worldwide Logistics by e-mail or phone.

8. Whistleblowing

AIT Worldwide Logistics has implemented a Whistleblowing Reporting System in accordance with the EU Directive 2019/1937 on the protection of persons who report breaches of Union Law (“Whistleblowing Directive”) and relevant national laws (national transposition measures). The list of the relevant national laws is available under: https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=celex:32019L1937.

When making a report, the following categories of personal data may be collected and processed:

- Identification data and contact details (unless you report anonymously);
- Whether you are employed by AIT Worldwide Logistics;
- Identification data of the persons you name in your report if you provide such information; and
- Description of the alleged misconduct as well as a description of the circumstances of the incident.

The legal basis for collecting and processing your personal data is Art. 6(1)(c) of GDPR, namely our legal obligation to implement internal reporting channels (Art. 8 of the EU Whistleblowing Directive and its transposed national laws, and Art. 6(1)(f) of GDPR, namely our legitimate interest in preventing, detecting, investigating and addressing alleged violations or breaches.

The Whistleblowing Reporting System is available here. Please note, that the administrator of the Whistleblowing Reporting System is an external service provider: NAVEX Global Inc., who acts as Processor and that a corresponding Data Processing Agreement has been concluded.

Please also note, that your personal data may be transferred to the United States. NAVEX Global Inc. has, however, taken part to the EU-US Data Privacy Framework, which enables the transfer of personal data from Europe to the United States and additional Standard Contractual Clauses pursuant to Art. 46 GDPR have been concluded. More information on how NAVEX Global Inc. processes your personal data can be found in their privacy policy, available here.

Your personal data will be kept no longer than 3 years after the end of each investigation on the alleged violation or breach. Longer storage periods may be necessary due to mandatory legal obligations arising from, for example, criminal procedure, legal claims, occupational safety laws, etc.

9. Handling of Data Privacy Requests

If you submit a request to us or to our Data Protection Officer, (e.g. you exercised one of your Data Privacy Rights), we may process the following categories of personal data:

- Identification data; and
- Contact details.

Please note, that depending on the request, additional categories of personal data may be processed.

We will exclusively process your personal data for handling your request and to provide you with the required information. Depending on your request, your information may be shared with:

- Our European Data Protection Officer (2B Advice GmbH);
- Other entities belonging to the AIT Worldwide Logistics group of companies; and
- Third-Parties, to whom we provided your personal data (e.g. Processors / Service Providers).

The legal basis for processing your personal data is Art. 12 seq. GDPR / UK GDPR and Art. 25 seq. of the Swiss Data Protection Law. Please note, that for internal documentation purposes, your request and your information will be kept by us 6 years.

10. Handling of Data Breaches

A data breach is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

According to Art. 34 GDPR, Art. 34 UK GDPR and Art. 24 (4) of the Swiss Data Protection Law, we may need to inform you of the occurrence of a data breach in case your personal data has been compromised. In that case, we may process the following personal data concerning you:

- Identification data;
- Contact details; and
- Other data concerning you, that may have been compromised.

We will process your data exclusively to inform you on the data breach, to describe you the likely consequences of the personal data breach, describe the measures taken or proposed to be taken by us to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. Your personal data may be shared internally with the relevant departments responsible for handling data breaches (e.g. IT department, HR department, etc) and with our external Data Protection Officer (2B Advice GmbH). We may also forward your personal data if required by a Supervisory Authority.

We will keep communication with you and all related documents for a period of 6 years to demonstrate compliance with our legal obligations.

11. Managing Business Relationships

For the purpose of managing business relationships with our clients, suppliers, vendors or any kind of third party involved in a business relationship with us, we may process the following categories of personal data:

- Identification data;
- Contact details;
- Company data;
- Business / Professional data;
- Contractual data;
- Communication data;
- Financial data; and
- Insurance data.

The terms “Managing Business Relationship” may include the following processing activities: facilitating communication with you; processing financial transactions, billing, payments, and related financial activities necessary for our collaborations; responding to your inquiries, questions, or requests; providing you access to “My AIT”; handling a complaint, etc.

We process your data to enter in a contract with you or to execute our contractual obligations.

We may also use your information for marketing purposes (e.g. sending you newsletter or information on new products, ask you to answer a survey, etc). In that case, the legal basis for processing your data is our legitimate interests.

Your personal data will be kept by us at least until the end of our business collaboration. Please note, that we are obliged by law to keep some categories of personal data and documents (e.g. invoices, contracts, etc.) even if the purposes for which the data has been collected, has been achieved. For more information, please contact our external Data Protection Officer.

12. Pay Invoice with Credit Card

You have the possibility to pay invoices with a credit card via a third-party link provided on our website: SlimCD - AIT Credit Card Payment Processing.

Your payment information will be processed by our payment service provider Slim CD. This service provider may process the following categories of personal data:

- Payment information (Card number, expiration date, CVV2);
- Billing information (Customer code, Identification data, Billing address, E-Mail Address); and
- Invoice number(s).

Your payment information will be processed for the purpose of payment processing (execution of a contract). For more details on how Slim CD processes your information please check their website (https://slimcd.com/) or their privacy policy available here.

13. Social Media: LinkedIn, Facebook, & Youtube

AIT Worldwide Logistics maintains presence on the following social media platforms:

Facebook

https://www.facebook.com/AITWorldwide

LinkedIn

https://www.linkedin.com/company/ait-worldwide-logistics/

https://www.linkedin.com/showcase/ait-worldwide-logistics-careers/

https://www.linkedin.com/company/ait-home-delivery/

Youtube

https://www.youtube.com/@AITWORLDWIDELOGISTICS

On these different social media platforms, you have the possibility to “follow” us, comment and / or share our posts or directly interact with us. When interacting with us, we may process the following categories of personal data:

- Identification data (name, surname or nickname);
- Contact details (e.g. your social media profil, your E-Mail Address); and
- Personal data contained in the messages you send to us.

The processing of your personal data is based on our legitimate interest in interacting with you or in answering your request.

Please note, that from a data protection point of view, we act as joint-controllers together with LinkedIn Ireland Unlimited Company (service provider of LinkedIn), Meta Platforms Ireland Limited (service provider of Facebook) and Google LLC (service provider of Youtube) and that corresponding agreements have been concluded. They are available under:

- LinkedIN: LINK

- Facebook: LINK
- Google: LINK

Additional categories of personal data may be processed by service providers of the social media platforms for marketing and analytical purposes (e.g. track your behavoir). We do not, however, have any information on how they use your personal data when you visit our social media pages and have no influence on the storage period of your data, which is stored by the service providers of the social media platforms.

For more details, please refer to their privacy policies:

- LinkedIN: LINK
- Facebook: LINK
- Youtube: LINK

Please also note, that your personal data may be transferred and further processed to third countries (e.g. United States). LinkedIn Corporation, Meta Platforms Inc. and Google LLC have however taken part to the EU-US Data Privacy Framework, which enables the transfer of personal data from Europe to the United States.

14. Use of Google Analytics

Our Site uses functions of the web analysis service Google Analytics either directly in your browser (client-side tracking) or indirectly on our webserver (server-side tracking). The provider is Google Ireland Limited ("Google"), Gordon House, Barrow Street, Dublin 4, Ireland. Google Analytics enables website operators to analyze the behavior of visitors.

Website operators receive various usage data, such as page views, length of stay, operating systems used and origin of the user. This data may be summarized by Google in a profile that is assigned to the respective user or their device.

The aim of using Google Analytics is to recognize the user or visitor for the purpose of analyzing his or her behavior when he or she visits or uses our Site. The information collected by Google about the use of our Site is usually transmitted to a Google server in the United States and stored there.

The use of Google Analytics is based on your consent. When you visit our Site, a cookie banner appears. If you accept the use of non-essential cookies, we will process your data for analytical purposes. Please note, that at any time, you have the right to revoke your consent or to manage your preferences. To do so, please click on the Cookie icon at the bottom of the website of the left side.

Please note, that your information may be transferred to the United States by Google. Google has taken part in the EU-US Data Privacy Framework enabling the transfer of personal data from Europe to the United States.

You can learn more about Google's use of data, as well as available settings and opt-out options at: https://www.google.com/intl/de/policies/privacy/partners "Use of data by Google when using the websites or apps of our partners"), https://www.google.com/policies/technologies/ads ("Use of data for advertising purposes), https://www.google.de/settings/ads ("Managing information that Google uses to show you advertising").

15. Use of Google Ads

We use Google Ads, a service provided by Google Ireland Limited, Google Building Gordon House, Barrow St, Dublin 4, Ireland. Google Ads enables us to use the information we collect (identification data, contact details or browser behavior) when you visit or interact with our Site for marketing and retargeting purposes.

Retargeting (or remarketing) is an online advertising method that allows us to reach out to previous visitors of our Site or to re-engage with potential customers. The legal base for processing your personal data is your consent. When you visit our Site, a cookie banner appears. If you accept the use of non-essential cookies, we will process your data for remarketing purposes. Please note, that at any time, you have the right to revoke your consent or to manage your preferences. To do so or to obtain more information on the cookies used for re-marketing purposes, please click on the Cookie icon at the bottom of the website of the left side.

Please note, that your information may be transferred to the United States by Google. Google has taken part in the EU-US Data Privacy Framework enabling the transfer of personal data from Europe to the United States.

You can learn more about Google's use of data, as well as available settings and opt-out options at: https://www.google.com/intl/de/policies/privacy/partners "Use of data by Google when using the websites or apps of our partners"), https://www.google.com/policies/technologies/ads ("Use of data for advertising purposes), https://www.google.de/settings/ads ("Managing information that Google uses to show you advertising").

16. Use of Chatbots (FreshChat, RingCentral Chat)

We use the chatbot systems Freshchat and RingCentral Chat, provided by Freshworks Inc. and RingCentral, Inc.. Please note that both service providers act as Processor –

which means that they process personal data on our behalf – and that Data Processing Agreements have been concluded to ensure the proper processing of your personal data.

These two systems are used by us for the purposes of communicating *via* live chat with interested parties, customers and business partners as well as website users. When interacting with them, the following categories of personal data may be processed: identification data, contact details, tracking number, content of the messages sent via the chatbot systems.

The legal base for processing the personal data is our legitimate interest in handling your request and in offering direct and effective customer communication that is easily accessible to every data subject. The information will be kept no longer than is necessary for achieving the purposes for which it has been collected (e.g. handling your request).

Please note, that your information may be transferred to a third-country and more specifically to the United States. However, Freshworks Inc. as well as RingCentral Inc. have taken part to the EU-US Data Privacy Framework enabling the transfer of personal data from Europe to the United States.

For more information, please visit the website of the service providers:

- Freshworks: www.freshworks.com
- RingCentral: www.ringcentral.com

17. Use of Microsoft Clarity

We improve our website by using Microsoft Clarity to see how you use our website. The legal base for processing the collected information is your consent. You can revoke your consent at any time by clicking on the Cookie icon.

Website usage data (e.g. behavioral metrics, clicks, scrolls, navigation) is captured using first and third-party cookies and other tracking technologies to determine the popularity of online activity. We inform you, that the personal data is collected by Microsoft Clarity.

For more information about how Microsoft collects and uses your data, visit the Microsoft Privacy Statement available under LINK.

General Information on the Disclosure of Your Personal Data

Except as set forth in this Global Privacy Policy, we will not disclose or sell your personal data. Personal information may occasionally be transferred to AIT's affiliates and to third parties who act for or on behalf of AIT or in connection with the business of AIT, for our administrative purpose including activities such as IT management, for us to provide Services to you, or to support and supplement the Services we provide. Such third parties may operate under different privacy policies.

AIT may disclose the personal data collected:

- where disclosure is necessary to comply with legal process (such as a court order, subpoena, search warrant, etc.) or other legal requirements of any governmental authority;
- where disclosure would potentially mitigate AIT's liability in an actual or potential lawsuit or claim;
- where disclosure is otherwise necessary to protect AIT's rights or property;
- where disclosure is necessary to protect the legal rights or property of others, including to protect the confidentiality or security of your personal information;
- as part of a bankruptcy, merger, reorganization, or a sale of the assets of AIT, a subsidiary, or division;
- where disclosure is necessary in connection with other business purposes including, without limitation, customer care, service quality, business management and operation, risk assessment, security, fraud and crime prevention/detection, monitoring, research and analysis, marketing, customer purchasing preferences, and trends and dispute resolution;
- where disclosure is necessary for us to provide it to our attorneys, accountants, regulators, auditors or other advisors; or
- where it is otherwise necessary for us to disclose it as required or permitted by law.

We may disclose your information with the following categories of third parties:

- user access, customer service, and quality assurance applications;
- customer service survey companies;
- shipping partners;
- marketing providers;
- data analytics, network monitoring services, and incident response providers;
- advisors such as lawyers, banks, accountants, auditors, and insurers;
- governmental and regulatory agencies;
- law enforcement, courts, and pursuant to legal process where required by law; and
- business partners such as investors or parties to merger and acquisition.

Children's Privacy

Our website is intended for a general audience, and we do not knowingly collect data about minors under 16 or sell products or Services to minors under 16. We do not knowingly collect personal data from anyone under the age of 16. If you are a parent or guardian and you are aware that your child has provided us with personal data, please email us at dataprivacyoffice@aitworldwide.com or aitworldwide@2b-advice.com (for European residents). If we become aware that we have collected personal data from minors under the age of 16 without verification of parental consent, we will take steps to delete that data.

Your Data Privacy Rights

You can assert your rights as a data subject with regard to your processed personal data at any time using the contact details of the Controller or the Data Protection Officer given above. As a data subject, you have the following rights:

Right to revoke consent: if personal data is processed on the basis of consent, you have the right to revoke this consent at any time for future processing.

Right to know if and what data we process: you can request confirmation of whether your data is being processed by us. If this is the case, we will provide you with information on what personal data we collect and how we process it.

Right to correct: if your personal data has been collected or processed while incorrect, you have the right, to request that this data be corrected immediately.

Right to delete: in certain circumstances, you have the right to request deletion of your personal data. Please note, that we usually delete your personal data if it is no longer necessary for achieving the original purpose of the processing. In some cases, and due to legal obligations to keep your personal data, we won't be able to delete your data.

Right to restriction of processing: you have the right to demand that the processing of your personal data be restricted.

Right to data portability: you have the right to receive a copy of the personal data you provided in a structured, commonly used and machine-readable format.

Right to object: if processing the personal data is necessary to safeguard the legitimate interests of our company, you can object to the processing at any time.

Right to file a complaint: you have the right to lodge a complaint with the competent supervisory or regulatory authorities.

For European residents, the main Data Protection Supervisory Authorities with which we cooperate in our respective jurisdictions are the following:

Germany

Landesbeauftragte für Datenschutz und Informationsfreiheit Nordhein-Westfalen

https://www.ldi.nrw.de/

Italy

Garante per la protezione dei dati personali

www.garanteprivacy.it

France

CNIL (Commission Nationale de l'Informatique et des Libertés)

www.cnil.fr

United Kingdom

Information Commissioner's Office

https://ico.org.uk/

Belgium

Autorité de protection des données

www.autoriteprotectiondonnees.be

Netherlands

Autoriteit Persoonsgegevens

https://www.rijksoverheid.nl

Czech Republic

Úřad pro ochranu osobních údajů

www.uoou.gov.cz

Switzerland

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter

www.edoeb.admin.ch

Changes to the Global Privacy Policy

This Global Privacy Policy is subject to occasional revision and we reserve the right, at our sole discretion, to change, modify, add, or replace any part of this Global Privacy Policy at any time for any reason. Each time you use the Site or the Services, the current version of the Global Privacy Policy will apply. Accordingly, your continued use of our Site or our Services following a change in this Global Privacy Policy represents your acceptance of the latest version to the fullest extent permitted by law. We suggest that you regularly review this Global Privacy Policy for changes and to ensure that you understand and accept our privacy practices and your obligations in accessing the Site and using our Services.

Addendum A: Additional Privacy Terms for Chinese Residents

This Addendum applies to the processing of personal information of residents of the People's Republic of China ("China", excluding, for the purposes of this Addendum, Hong Kong, Macau, and Taiwan). AIT Worldwide Logistics group of companies are committed to processing and protecting your personal data in accordance with Chinese laws and regulations, including the Personal Information Protection Law of China ("PIPL").

For Chinese residents, this Addendum supplements AIT Worldwide Logistics' Global Privacy Policy. In the event of any inconsistency between the terms of this Addendum and those in the Global Privacy Policy, the terms of this Addendum shall prevail in the context of processing personal information of Chinese residents.

This Addendum is intended to inform you, prior to or at the time of providing us with your personal information, about why and how we process your personal information.

The term "personal information" as used in this Addendum refers to any information recorded electronically or otherwise that relates to an identified or identifiable natural person, excluding anonymized information. Unless otherwise specified, the definitions of terms in this Addendum are consistent with the meanings in AIT Worldwide Logistics' Global Privacy Policy.

Contact details of the Controller

AIT Worldwide Logistics (Shanghai) Ltd.
Room 1006-1010, Ruifeng International Building
No. 248, YangShuPu Road
200082 Shanghai
Peoples Republic of China
Email: dataprivacyoffice@aitworldwide.com

On What Basis Do We Process Your Information?

We process your personal information for the purposes stated based on one or more of the following legal bases:

- Your consent;
- Processing is necessary for the conclusion or performance of a contract to which you are a interested party, or for human resource management according to lawfully formulated labor rules and structures and lawfully concluded collective contracts;
- Processing is necessary for compliance with legal or regulatory obligations to which we may be subject;

- Processing is necessary to respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property, under emergency conditions;

- Processing is necessary within a reasonable scope to implement news reporting, public opinion supervision, and other such activities for the public interest.

Where Do We Process Your Personal Information?

Please understand that AIT Worldwide Logistics is a global company headquartered in the USA. Within the scope permitted by the PIPL, we may transfer your personal information to our affiliates and subsidiaries in the USA and other countries / region (e.g. Europe) for business operations, corporate governance, and other purposes. We will obtain your separate consent for such transfers.

We may also transfer your personal information to third-party service providers and business partners in different countries to improve operational efficiency and performance, and to create backups for business continuity and disaster recovery purposes. We will ensure that the recipient is subject to applicable laws within its jurisdiction that provide protection standards equivalent to those under this Addendum.

We will notify you, in accordance with applicable laws and regulations, of the name, contact information, processing purpose, processing methods, the type of personal information being transferred, and the methods and procedures for exercising your rights under the PIPL against the overseas recipient, and obtain your separate consent before transferring your personal information abroad. You may withdraw your consent at any time.

Additionally, we will take all reasonable measures to ensure that the cross-border transfer of your personal information complies with applicable legal and regulatory requirements, including but not limited to completing a personal information protection impact assessment, passing security assessments, and signing standard contracts where necessary.

Your Privacy Rights

If you wish to exercise your rights under the PIPL within the limits allowed by law (including but not limited to the right to access and copy, the right to rectification, the right to deletion, and the right to data portability), or if you have any questions about this Addendum or how we use your personal information, please contact us at: dataprivacyoffice@aitworldwide.com or aitworldwide@2b-advice.com.

You have the right to lodge a complaint with the Cyberspace Administration of China or other applicable data protection authorities.

Minors Under the Age of 14

Our website is not intended for children under the age of 14, and we do not knowingly collect personal information from children under 14. If we are informed that we have

collected or received personal information from a child under the age of 14, we will delete that information.

Changes to This Addendum

We reserve the right to amend this Addendum at any time. If we make changes to this Addendum, we will post the updated Addendum on our website and update the effective date of the Addendum. Your continued use of our website after the changes have been posted signifies your acceptance of such changes.

Addendum B:
Additional Privacy Terms for Residents of the United States of America

This Addendum applies to the processing of personal data of residents of the United States of America and supplements AIT Worldwide Logistics' Global Privacy Policy.

In the event of any inconsistency between the terms of this Addendum and those in the Global Privacy Policy, the terms of this Addendum shall prevail in the context of processing personal data of residents of the United States of America.

Effective Date: November 13, 2026

Sources of Personal Data We Collect

We gather your data on our Services depending on the type of interaction you have with us, for example via your interaction with our Services such as scheduling a shipment, sending us an email, and customer service calls; or when you apply for a job with us.

We collect personal data from third-party sources (including recruiters), or from publicly available sources, such as search engines, public databases, etc.

We gather data on our Site from users by tracking pages visited and collecting information from voluntary submissions. We may use various technologies as well (e.g., cookies) to collect data from your computer and about your activities on our Site. We collect aggregate data regarding which pages of our Site's users access or visit. For more information, see the **Personal Data We Collect and Process, and the Applicable Purposes** section in the Global Privacy Policy.

Categories of Personal Data We Collect

Depending on our relationship with you, we may collect the following categories of personal data about you:

- "Sensitive Personal Information" such as Social Security numbers (SSNs), Driver's license, financial account or card numbers, Precise geolocation, Racial and ethnic characteristics, or biometric information.
- "Identifiers" such as name, alias, address, unique identifier, internet protocol address, email address, telephone number, financial account number, financial information, education or employment history, medical information, health insurance information, Social Security Number, or government identification number;
- "Other Personal Information" such as name, signature, Social Security Number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information. Some personal information included in this category may overlap with other categories;

- "Protected Characteristics" under California or federal law for classifications such as age (40 years or older), race, color, ancestry, national origin, citizenship, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, gender expression, pregnancy or childbirth and related medical conditions), sexual orientation, or veteran or military status;
- "Commercial Information" such as records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies;
- "Internet or Network Activity" such as browsing history, search history, information on a consumer's interaction with a website, application, or advertisement;
- "Geolocation" such as physical movements or location;
- "Sensory Data" such as audio, electronic, or visual information when you participate in telephone screens or video interviews with us or appear in security footage;
- "Professional or Employment Related Information" such as current or past job history or performance evaluations;
- "Biometric Information" such as physiological, biological, or behavioral characteristics, including information that is used or is intended to be used singly or in combination with each other or with other identifying data, to establish individual identity; imagery of the face from which an identifier template, such as a faceprint can be extracted. For more information on the Biometric Information we collect, see our Biometric Privacy Policy; and
- "Inferences" such as profile reflecting a person's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

Use of Personal Data

We may use any personal data collected pursuant to this Privacy Policy:

- To provide our Services to you;
- To manage our Site;
- To measure and improve those Services;
- To develop internal and external analyses;
- To contact you or, if applicable, your designated representative(s) by post, telephone, electronic mail, facsimile, etc., in connection with your account or shipment;
- To process your job application and administer your employment;
- To provide and administer employment benefits and provision payroll;

- To evaluate your job performance
- To facilitate our internal business operations, including assessing and managing risk and fulfilling our legal and regulatory requirements;
- To administer, operate, facilitate, and manage your relationship and/or account with us. This may include sharing such information internally, as well as disclosing it to our affiliates or other third parties;
- To protect our users and provide them with customer support;
- To provide you with news, special offers, marketing and promotional materials and general information about other services and events which we offer that are similar to those that you have already purchased or inquired about or otherwise might be interested in, unless you have opted not to receive such information;
- To audit downloads of information from our Site and also make follow-up contact with you by email in relation to the material you have accessed;
- To prevent and prosecute fraud, including through the identification of drivers or visitors on AIT property;
- To protect our legal rights and the legal rights of others; and
- Other purposes you consent to, are notified of, or are disclosed when you provide personal data.

For additional details, see **Personal Data We Collect and Process, and the Applicable Purposes** in the Global Privacy Policy.

We may also disclose or process de-identified information for legitimate and lawful business purposes. Where we have de-identified data, we will maintain and use it without attempting to re-identify the data other than as permitted under law.

We do not use sensitive personal information to infer characteristics about our business contacts or outside of legally permitted purposes.

Disclosure of Personal Data

Personal information may occasionally be transferred to AIT affiliates and to third parties who act for or on behalf of AIT or in connection with the business of AIT, for our administrative purpose including activities such as IT management, for them to provide services to you, or to support and supplement the Services we provide. Such third parties may operate under different privacy policies. AIT may disclose the personal information collected (i) where disclosure is necessary to comply with legal process (such as a court order, subpoena, search warrant, etc.) or other legal requirements of any governmental authority; (ii) where disclosure would potentially mitigate AIT liability in an actual or potential lawsuit; (iii) where disclosure is otherwise necessary to protect AIT rights or property; (iv) where disclosure is necessary to protect the legal rights or property of others, including to protect the confidentiality or security of your personal

information; (v) as part of a bankruptcy, merger, reorganization, or a sale of the assets of AIT, a subsidiary, or division; (vi) where disclosure is necessary in connection with other business purposes including, without limitation, customer care, service quality, business management and operation, risk assessment, security, fraud and crime prevention/detection, monitoring, research and analysis, marketing, customer purchasing preferences, and trends and dispute resolution; (vii) where disclosure is necessary for us to provide it to our attorneys, accountants, regulators, auditors or other advisors; or (vii) where it is otherwise necessary for us to disclose it as required or permitted by law.

We may disclose your information with the following categories of third parties:

- With user access, customer service, and quality assurance applications we disclose Identifiers and Other Personal Information.
- With customer service survey companies we disclose Identifiers and Other Personal Information.
- With shipping partners we disclose Identifiers and Other Personal Information.
- With marketing providers we disclose Identifiers and Other Personal Information.
- With our data analytics, security vendors, network monitoring services, and incident response providers, we disclose Sensitive Personal Information, Identifiers, Other Personal Information, Protected Characteristics, and Biometric Information.
- With our clients or business partners for the prevention of fraud and driver identity verification, we disclose Sensitive Personal Information, Identifiers, Other Personal Information, Protected Characteristics, Biometric Information, Geolocation, Sensory Data, and Professional or Employment Related Information.
- With our advisors such as lawyers, banks, and insurers, we disclose Sensitive Personal Information, Identifiers, Other Personal Information, Protected Characteristics, Commercial Information, Internet or Network Activity, Biometric Information, Geolocation, Sensory Data, Professional or Employment Related Information, and Inferences.
- With our governmental and regulatory agencies, we disclose Sensitive Personal Information, Identifiers, Other Personal Information, Protected Characteristics, Commercial Information, Internet or Network Activity, Biometric Information, Geolocation, Sensory Data, Professional or Employment Related Information, and Inferences.
- With law enforcement, government entities, courts, and pursuant to legal process where required by law, we disclose Sensitive Personal Information, Identifiers, Other Personal Information, Protected Characteristics, Commercial Information, Internet or Network Activity, Biometric Information, Geolocation, Sensory Data, Professional or Employment Related Information, and Inferences.

- With business partners such as investors or parties to merger and acquisition, we disclose Sensitive Personal Information, Identifiers, Other Personal Information, Protected Characteristics, Commercial Information, Internet or Network Activity, Biometric Information, Geolocation, Sensory Data, Professional or Employment Related Information, and Inferences.

Online Tracking Technology – Right to Opt Out

We allow certain third parties to use cookies and other online tracking technologies to collect personal information on our Sites to personalize your experience, provide free or enhanced add-on services to our company, to facilitate our marketing and advertising, and use your personal information for purposes beyond the services they provide to our company (for example, building consumer profiles to help other clients with their targeted advertising or enriched analytics). These types of online disclosure of personal information may be defined as "sales" or "sharing" under applicable law(s). We may "sell" or "share" the following categories of personal information to third party online analytics and advertising providers: personal identifiers; internet and network information; corporate affiliation information (to the extent it can be derived from your activity on our Sites).

You have the right to, and may, opt out of such "sale" or "sharing" by using GPC signals. For more information on how to use GPC signals, visit www.globalprivacycontrol.org.

For additional details on how to manage your preferences, see **Personal Data We Collect and Process, and the Applicable Purposes** in the Global Privacy Policy and the Consent Management Tool at the bottom of the website of the left side.

Additional Data Privacy Rights

See "**Your Data Privacy Rights**" in the Global Privacy Policy for detail on your privacy rights and how to make a request.

Right to Limit the Use of Sensitive Personal Data: You have the right to direct a business that collects your sensitive personal information to limit its use to uses which are necessary to perform the services or provide the goods reasonably expected. However, we only uses Sensitive Personal Information to provide the Services requested by you; to prevent, detect, and investigate security incidents; to resist malicious, deceptive, fraudulent, or illegal actions and to prosecute those responsible for such actions; to ensure people's physical safety; to perform services on our behalf; to verify or maintain the quality or safety of our products, services, and devices.

Right of Non-Discrimination: You have the right not to receive discriminatory treatment by us when you exercise your privacy rights.

Right to Appeal: In certain cases, you have the right to appeal if we deny your privacy request. If your request is denied, we will provide additional instructions on the appeals

process. Please contact dataprivacyoffice@aitworldwide.com if you wish to appeal. We will consider your request and applicable law and notify you of our decision.

Retention of Personal Information

We will retain your personal data as necessary to fulfil the purposes outlined in this Global Privacy Policy unless otherwise required by law. The criteria used to determine the retention periods include: (i) how long the personal data is needed to provide the services and operate the business; (ii) the type of personal data collected; and (iii) whether we are subject to a legal, contractual or similar obligation to retain the personal information (e.g., mandatory data retention laws, government orders to preserve data relevant to an investigation, or data that must be retained for the purposes of litigation or disputes).

If your relationship with us ends, we will continue to treat your personal data, to the extent we retain it, as described in this **Global Privacy Policy**.

Your Communication Choices

General: You have certain choices about communication using your personal information. Where you have consented to the processing of your personal information, you may withdraw that consent at any time and prevent further processing by contacting us as described below. Even if you opt out, we may still collect and use non- personal information regarding your activities on our Sites and for other legal purposes.

Email and Telephone Communications: If you receive an unwanted email from us, you can use the unsubscribe link found at the bottom of the email to opt-out of receiving future emails. Note that you will continue to receive transaction-related emails regarding Services you request. We may also send you certain non-promotional communications regarding us and our Services, and you will not be able to opt out of those communications (e.g., communications regarding our Services or updates to our Terms of Use or this Global Privacy Policy).

We process requests to be placed on do-not-mail, do-not-email, and do-not-call lists as required by applicable law.

Mobile Devices: We may send you push notifications through our mobile application(s). You may at any time opt-out from receiving these types of communications by changing the settings on your mobile device. With your consent, we may also collect location-based information if you use our mobile applications. You may opt-out of this collection by changing the settings on your mobile device.

Shine the Light

Pursuant to Section 1798.83 of the California Civil Code, residents of California have the right to request from a business, with whom the California resident has an established business relationship, what types of personal information the business shares with third

parties for direct marketing purposes by such third party and the identities of the third parties with whom the business has shared such information in the immediately preceding calendar year. To access this information, please contact us by email at dataprivacyoffice@aitworldwide.com including "Shine the Light Privacy Request" in the subject line or mail at 2 Pierce Place, Suite 2100, Itasca, IL 60143, Attn: Shine the Light Privacy Request.

Minors

We do not sell the personal information and do not have actual knowledge that we sell the personal information of minors under 16 years of age. If we wish to do so in the future, we will first seek affirmative authorization form either the minor who is between 13 and 16 years of age, or the parent or guardian of a minor less than 13 years of age. Please contact us at dataprivacyoffice@aitworldwide.com to inform us if you, or your minor child, are under the age of 16.

If you are under the age of 18 and you want to remove your name or comments from our website or publicly displayed content, please contact us directly at dataprivacyoffice@aitworldwide.com. We may not be able to modify or delete your information in all circumstances.

If you wish to submit a privacy request on behalf of your minor child in accordance with applicable jurisdictional laws, you must provide sufficient information to allow us to reasonably verify your child is the person about whom we collected personal information and you are authorized to submit the request on your child's behalf (i.e., you are the child's legal guardian or authorized representative).

Do Not Track Signals

AIT does not respond to Do Not Track signals sent by your web browser because a uniform technological standard has not yet been developed. Our Site does, however, honor Global Privacy Control signals. For more information on how to utilize that tool, visit www.globalprivacycontrol.org.

Addendum C:
U.S. Biometric Privacy Policy

AIT Worldwide Logistics, Inc. ("AIT") has instituted the following biometric information privacy policy. This policy supplements AIT's Global Privacy Policy (www. https://www.aitworldwide.com/privacy-policy/).

Biometric Data Defined

As used in this policy, biometric data includes "biometric identifiers" and "biometric information" as defined in the Illinois Biometric Information Privacy Act, 740 ILCS § 14/1, et seq. "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996.

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

Purpose for Collection of Biometric Data

AIT, its vendors, and/or the licensor of AIT's yard management software collect, store, and use biometric data solely for driver and visitor identification, fraud prosecution and prevention, and to execute a security threat assessment.

Disclosure and Authorization

To the extent that AIT, its vendors, and/or the licensor of AIT's yard management software (Renaissant, Inc.) collect, capture, or otherwise obtain biometric data relating to a driver or visitor, AIT must first:

a. Inform the driver or visitor in writing that AIT, its vendors, and/or the licensor of AIT's yard management software are collecting, capturing, or otherwise obtaining that person's biometric data, and that AIT is providing such biometric data to its vendors, the licensor of AIT's yard management software and law enforcement;

b. Inform the driver or visitor in writing of the specific purpose and length of time for which the driver or visitor's biometric data is being collected, stored, and used; and

c. Receive a written release signed by the driver or visitor (or his or her legally authorized representative) authorizing AIT, its vendors, and/or the licensor of AIT's yard management software to collect, store, and use the driver or visitor's biometric data for the specific purposes disclosed by AIT, and for AIT to provide such biometric data to its vendors, the licensor of AIT's yard management software and law enforcement.

AIT, its vendors, the licensor of AIT's yard management software and law enforcement will not sell, lease, trade, or otherwise profit from driver or visitor's biometric data; provided, however, that AIT's vendors, the licensor of AIT's yard management software and law enforcement may be paid for products or services used by AIT that utilize such biometric data.

Disclosure

AIT will not disclose or disseminate any biometric data to anyone other than its vendors, the licensor of AIT's yard management software and law enforcement without/unless:

a. First obtaining written consent to such disclosure or dissemination;

b. The disclosed data completes a financial transaction requested or authorized by the driver or visitor;

c. Disclosure is required by state or federal law or municipal ordinance; or

d. Disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

Retention Schedule

AIT shall retain the driver or visitor's biometric data only until, and shall request that its vendors, the licensor of AIT's yard management software and law enforcement permanently destroy such data within 3 years of the driver or visitor's applicable visit (resulting in biometric collection) with AIT.

Data Storage

AIT shall use a reasonable standard of care to store, transmit and protect from disclosure any paper or electronic biometric data collected. Such storage, transmission, and protection from disclosure shall be performed in a manner that is the same as or more protective than the manner in which AIT stores, transmits and protects from disclosure other confidential and sensitive information, including personal information that can be used to uniquely identify an individual or an individual's account or property, such as genetic markers, genetic testing information, account numbers, PINs, driver's license numbers and social security numbers.

Addendum D:
List of Additional Controllers

1. AIT Blockchain Solutions LLC
2. AIT Buyer LLC
3. AIT Customs Brokerage, Inc.
4. AIT Euro Holding B.V.
5. AIT Global LLC
6. AIT Holdco, Inc.
7. AIT Home Delivery GmbH
8. AIT Home Delivery UK Ltd.
9. AIT Home Delivery, LLC
10. AIT Marine Logistics Denmark ApS
11. AIT Truckload Solutions, Inc.
12. AIT TW Worldwide Logistics, Ltd.
13. AIT UK Acquisition Company Limited
14. AIT UK Holdings Limited
15. AIT Worldwide Logistics (Canada), Inc.
16. AIT Worldwide Logistics (M) SDN. BHD.
17. AIT Worldwide Logistics (Shanghai) Ltd.
18. AIT Worldwide Logistics (UK) Limited
19. AIT Worldwide Logistics Australia Pty Ltd
20. AIT Worldwide Logistics B.V.
21. AIT Worldwide Logistics Belgium N.V.
22. AIT Worldwide Logistics Czech Republic s.r.o
23. AIT Worldwide Logistics Denmark ApS
24. AIT Worldwide Logistics Germany GmbH
25. AIT Worldwide Logistics Germany GmbH - Austria Branch
26. AIT Worldwide Logistics Holdings, Inc.
27. AIT Worldwide Logistics India Private Ltd.
28. AIT Worldwide Logistics Intermediary Holdings, Inc.
29. AIT Worldwide Logistics Ireland Limited
30. AIT Worldwide Logistics Israel LTD.
31. AIT Worldwide Logistics Italy Srl
32. AIT Worldwide Logistics Korea, LLC
33. AIT Worldwide Logistics Marine (S) Pte. Ltd.
34. AIT Worldwide Logistics Middle East - L.L.C - S.P.C
35. AIT Worldwide Logistics Middle East FZE
36. AIT Worldwide Logistics Norway AS
37. AIT Worldwide Logistics Poland sp. z o.o.
38. AIT Worldwide Logistics SARL
39. AIT Worldwide Logistics Singapore Pte. Ltd.
40. AIT Worldwide Logistics Switzerland AG
41. AIT Worldwide Logistics Transport Limited Sti.
42. AIT Worldwide Logistics UAE B.V. - Dubai Branch
43. AIT Worldwide Logistics UAE B.V.
44. AIT Worldwide Logistics Vietnam Company Ltd.
45. AIT Worldwide Logistics, Ltd.
46. AIT Worldwide Logistics, S. de R.L. de C.V.
47. Cargo Zone LLC
48. Compass Cargo AG
49. Connor Anderson International Pty Ltd
50. Connor Anderson International Trust
51. Door to Deck Global Logistics Services Ltd.
52. Fiege Far East Holding LTD
53. Fiege Ltd.
54. Freight Agency Services, Inc.

55. Freight Empire S.A.S.
56. GB AIT Buyer, Inc.
57. GB AIT Holdco, Inc.
58. GB AIT Intermediateco, Inc.
59. GB AIT Topco, L.P.
60. Go Configure, LLC
61. Ingleby (2016) Limited
62. Innovative Delivery & Logistics, LLC
63. Intelligent Logistics LLC
64. Lubbers (UK) Ltd.
65. Lubbers @work B.V.
66. Lubbers Benelux B.V.
67. Lubbers Denmark ApS
68. Lubbers Germany GmbH
69. Lubbers Global Freight B.V.
70. Lubbers Global Freight UK Ltd.
71. Lubbers Italy srl
72. Lubbers Projects & Services B.V.
73. Lubbers Projects B.V.
74. Lubbers Romania srl
75. Lubbers Transport Group B.V.
76. Mach II Shipping Limited
77. Marine Trans USA LLC
78. Marinetrans AS
79. Marinetrans Benelux B.V.
80. Marinetrans China Co., Ltd.
81. Marinetrans Germany GmbH
82. Marinetrans Greece I.K.E.
83. Marinetrans Holding AS
84. Marinetrans Holding B.V.
85. Marinetrans Japan Co. Ltd.
86. Marinetrans Korea Co. Ltd.
87. Marinetrans Singapore Pte. Ltd.
88. mertus 686. GmbH
89. Pharmafreight Limited
90. PM USA, Inc.
91. Priano Marchelli SpA
92. Priano Marchelli USA, LLC
93. PT AIT Worldwide Logistics
94. SEL Holdings, LLC
95. Ship Spares Logistics B.V.
96. ShipSpare Forwarder Marinetrans Pvt. Ltd.
97. Spur Freight Services Inc.
98. T.L.K. Air Care, Inc.
99. Unitrans Holdings, Inc.
100. Unitrans International Corporation
101. Unitrans, Inc.
102. WC Logistics, Inc.