PRIVACY POLICY

EUROASIA TOTAL LOGISTICS PUBLIC COMPANY LIMITED

ISSUE 2

EFFECTIVE DATE 6 AUGUST 2022

Preparation and Approval History

Document No.	Editor/Controller	Reviewer	Approver
CP-BOD-014-02	Managing Director	Chief Executive Officer	Board of Directors
	10 June 2022	10 June 2022	5 August 2022

Revision History

Issue	Issue Date	Effective Date	Revision details
1	10 October 2021	9 November 2021	First issue
2	10 June 2022	6 August 2022	Revise company name after conversion to public limited company

Note: To add or cancel any document, proceed according to the acts set out in the Approval and Implementation Authority.

Euroasia Total Logistics Public Company Limited
19, 21 Motorway Road, Klongsongtonnoon,
Lat Krabang, Bangkok, 10520 Thailand
Tel: (662) 123 1727
Website: www.etl.co.th

บริษัท ยูโรเอเชีย โทเทิล โลจิสติกส์ จำกัด (มหาชน)
19, 21 ถนนมอเตอร์เวย์ แขวงคลองสองต้นนุ่น
เขตลาดกระบัง กรุงเทพมหานคร 10520
โทรศัพท์: (662) 123 1727
เว็บไซต์: www.etl.co.th

Privacy Policy

1. General Principle

1.1 Generality

Euroasia Total Logistics Public Company Limited (**"the Company"**) and its subsidiaries are committed to conducting business in accordance with the provisions of relevant laws, in particular attaching importance to the protection of personal data of stakeholders with the Company's business operations. The Company has developed a personal data management system with a modern operating system and information technology system that is secure and safe to effectively protect the privacy of personal information by requiring only the Company's staff or related persons to have the right to access personal information. In addition, the Company also establishes a system to strictly monitor the access and use of personal data, and regularly improves and develops the storage and retention system of personal data to make the storage system accurate and reliable and to prevent the leakage of personal information, personal data correction by a person not having a duty involved, or the use of personal information other than the purpose that the Company has earlier notified stakeholders.

This document describes the types of personal data and the purposes for which they are collected for the use or disclosure of personal data, data collection period, type of person or entity in which the Company may disclose personal information collected by the Company, rights of personal data owners, including measures to maintain the security of personal data in accordance with the provisions of the law as well as other information related to the Company's personal data management.

This document is also an integral part of the Company's terms and conditions of use of various services. The Company may amend, improve, add, or modify this policy and will notify employees and ask for their consent as specified by relevant personal data protection laws.

1.2 Definitions

To provide clarity in communication with stakeholders in the business and avoid any concerns about interpretation of certain terms in this document, the Company has prepared the definitions as follows:

"Company" means Euroasia Total Logistics Public Company Limited and its subsidiaries and includes one or more persons who are authorized to act on behalf of the Company and its subsidiaries.

"Personal Data" means information relating to an ordinary individual that enables to identify an individual either directly or indirectly.

"**Sensitive Personal Data**" means personal data about race, ethnicity, political opinion, cult, religion or philosophy beliefs, sexual behavior, criminal record, disability health information, labor union information, genetic data, biological data, or any other information that affects the owner of personal data in a similar way as determined by the Board of Directors.

"**Personal Data Controller**" means a person or a legal entity who has the authority to make decisions about the collection, use, or disclosure of personal data.

"**Personal Data Processor**" means a person or legal entity who performs collection, use, or disclosure of personal data by the order or on behalf of the personal data controller. However, the said person or juristic person is not a controller of personal data.

2. Collection Limitation Principle

2.1 Collected, Used or Disclosed Personal Data

This policy applies to personal data that the Company may collect, use, or disclose, including in the event that the data owner has given consent to the Company regarding the information as follows:

(a) General personal data, such as name, surname, date of birth, ID card number, address according to ID card, domicile address, current address, phone number, mobile phone number, family status, electronic mail account, photo on ID card, laser number on the back of the ID card.

(b) Sensitive personal data, for example, information about nationality, religion, blood type, health check-up results, medical history, diagnosis results, health information, criminal history, face, eyes, or fingerprint scan image.

(c) Other personal data, such as work history, car registration, motorcycles registered with government agencies, product reference number registered by the product user to guarantee that product or service, financial status, income, debt, consumption behavior, location of using the Company's services, and/or your interests in conjunction with other information that makes it possible to identify the person who is the owner of the data.

2.2 Collection and Acquisition of Personal Data

The Company adheres to the provisions of the law and collects personal data from the data owner only. Unless it is necessary that the data owner cannot or is not the one collecting such personal data, the Company may collect personal data from other sources. This will only apply in case the Company has obtained the written consent of the personal data owner. In general, the Company may collect personal data from other sources including:

2.2.1 Job Applicants or Employees

(a) Health-related personal data or congenital disease data of job applicants where the Company requires employees or staff do their own health check before the start of work by asking the hospital performing the health check to send the examination results of to the Company.

(b) Personal data relating to a history of legal action (criminal record) where the Company requires a criminal record check or to allow the Company to do a criminal background check on behalf of job applicants or employees.

(c) Personal information related to a previous work history before joining the Company where the Company requires the personal data owner to give expressive written consent to the Company first every time. The Company will notify the consent to such third parties to know in advance before sending such personal information to the Company.

2.2.2 Customers

In case personal data owners are interested in or order products from the Company, including contacting for after-sales service, the communication between customers and the Company, whether by phone, e-mail, the Company's application, applications used for communication, Customer Service Center, or contact by any other means, the Company may record such communications for various purposes, such as to use as evidence, to develop and improve the service, to track customers' satisfaction, to train personnel, to evaluate personnel performance, to analyze data, including to develop the Company's system.

3. Data Quality Principle

Before or while the Company collects, uses or discloses personal data of stakeholders, the Company has a process for managing and analyzing personal data based on the following principles:

- Accuracy
- Completeness
- Consistency
- Timeliness
- Uniqueness
- Validity

For the abovementioned process, the Company provides related persons to analyze and plan to collect particular data with uniqueness and accuracy suitable to processes for the use or disclosure of the personal data of the stakeholders with ultimate benefits. It also includes checking for correctness and accuracy of the data obtained before collection, whether recording information in the form of a book or an electronic system in order to be complete and correct. Besides this, the data will be verified from reliable sources or as agencies require by law to have the authority to manage personal data, including the protection of personal data, data safety and security to prevent it from being a legal and commercial claim in the future.

4. Purpose Specification Principle

The Company determines the objectives necessary to achieve the collective objectives in the provision of services and benefits to personal data owners classified by types of stakeholders and the Company's business operations as follows:

4.1 Shareholders

The Company will collect, use, or disclose personal data of the shareholders for the purpose of signing business contracts, general contracts, approval of various operations, authorization for business operations, law, transactions, banks, contacts with government agencies, general implementations in meeting invitations, notification of resolutions, dividend management, reports on the Company's performance according to regulations or as required by law.

4.2 Employees and Family Members

The Company will collect, use, or disclose personal information of employees in the scope of recruitment, selection, employment contract, identity verification, calculation and compensation payment, performance appraisal, wage adjustment, disciplinary conduct history collection and penalties, training, and personnel management as employees are employed by employment contracts, criminal record checks, job advancements, job position transfers, health checkup required by law and provided by the Company. It also includes the provision of welfare, benefits for employees and their families, and delivery of information to external agencies in compliance with the laws related to the Revenue Department and social security, labor skill development, the Legal Execution Department, and office administration, internal contacts and coordination, expense disbursement, property possession, premises administrative management, mail and postal management, recording of entry and exit of the work area, audits from both internal departments and external entities.

4.3 Partners

The Company will collect, use, or disclose personal data of partners that cover product owners, business partner, dealers, employers, as well as individuals who are required to fulfill partners' assignments in the scope of opening accounts for new receivables, quotations, negotiations, promotion activities, product launches, product demonstrations, sales management, advertising, reward payouts, sales returns and seller registration, procurement, seller evaluation, opening accounts for trade payables, and hiring contracts for services. In the case of being speakers or invited to give lectures or consultancy on the process of training, seminars, and meetings, a personal profile collected includes education, work experience, talents, and photos of activities. In the case of auditors from outside agencies, the Company will collect the particular personal information of auditors only for identity verification.

4.4 Customers

The Company will collect, use, or disclose personal information of customers for the benefit of customers starting from pre-sales service, trading, and after-sales service; review (expression of viewpoints, public relations, expression of emotion, notification of results of use of the goods and/or products), surveys, satisfaction, exchange of goods, customer complaint management, promotion presentation, notification of benefits to customers, satisfaction survey, organization of activities between customers and product owners (Brand) organized via Live or VDO conference systems, which the Company will collect, use, and disclose

personal information of those who participate in the activities according to the conditions set by the Company or product owners.

5. Use Limitation Principle

The Company will carefully consider the limited use of personal data of stakeholders within the scope of the purposes that were communicated to the stakeholders before or when collecting such personal data. In addition to awareness of privacy and fundamental rights of stakeholders as owners of personal data together with the provisions, rules, regulations, regulations, related governmental requirements, the Company will consider using personal information for the benefit or response to the stakeholders as customers, service recipients under the limited scope of the purpose for the following:

(a) Contacting to answer questions from customers

(b) Delivering products, services, or ordered products

(c) Managing and complying with contracts

(d) Supporting and maintaining products

(e) Conducting marketing research and development of new products and services

(f) Recommending marketing proposals and marketing communication

(g) Providing and communicating recruitment information to job applicants (including interns) and recruiting management of the Company

(h) Other purposes related to the above items. If personal data is acquired or used for purposes other than those stated above, consent is required before the acquisition or use of such information as necessary.

6. Security Safeguards Principle

The Company has established measures to maintain the security of personal data by taking into account the fundamental rights of the stakeholders' personal data. The Company has designed information systems and networking and computer systems to be as secure as possible to support the Company's continuous operations in accordance with the provisions of the relevant laws as well as preventing threats that may cause damage to the Company.

6.1 The Company has a duty to oversee that there is a written information technology security policy and must communicate the said policy to build understanding and be able to follow it properly, especially between the

Department of Information Technology and other departments within the company in order to have coordination and be able to operate the business according to the goals defined.

6.2 The Company regularly reviews the information technology security policy or when there are changes affecting the Company's information technology security.

6.3 The Company has designated persons with specific duties and responsibilities in managing information technology risks to ensure that the Company can provide information technology methods or approaches to reduce risks or manage existing risks and then presented them to the executives for consideration in information technology risk management.

6.4 The Company has identified risks related to information technology to cover key risks, such as:

(a) Personnel risk

(b) Software and data risks

(c) Network and internet risks

(d) Hardware and computer risks

(e) Financial risks

(f) Risk from floods and storms

(g) Risks from earthquake and building collapse

(h) Fire risks

(i) Theft risks

(j) Risks from power outages

6.5 The Company determines methods or tools for managing risks to an acceptable level. The Company prepares a table of descriptions and risks by having the titles, risk names, types of risks, risk characteristics, risk factors, and impacts, etc., and defines the level of the possibility of an incident and the severity of the risk impact, including charting risks.

6.6 The Company determines the indicators of the level of information technology risk and provides a monitoring system and reports results of the indicators to persons in charge to be able to manage risks appropriately and in a timely manner.

6.7 The Company prohibits its personnel from using the computer networks to act unlawful and contrary to good morals, such as creating a website to carry out trade or disseminate anything illegal or contrary to good morals.

6.8 The Company does not allow the use of computer networks or a computer with another user's account name both with and without permission from the owner of the user account name.

6.9 The Company prohibits access to the computer systems and information protected from access by others to modify, delete, add, or copy.

6.10 The Company prohibits the distribution of other people's information or the organization without permission from the information owners.

6.11 No one shall disrupt, obstruct, or damage the Company's resources and computer networks, such as transmitting a computer virus, entering a program that causes the computer or network devices to refuse to work.

6.12 No one is allowed to intercept information in the Company's computer network and of others in the process of receiving and sending in the computer networks.

6.13 Before using any portable media or opening files attached to electronic mails or files downloaded from the internet, users must check them for viruses with an antivirus program first every time.

6.14 The Company assigns duties to users in the Department of Information Technology responsible for maintaining the information systems used by the Company to ensure the security of the information systems and control operations in order to maintain the policy and practices in the security of the Company's information systems.

6.15 All employees of the Company must be responsible for complying with the Company's policy and practices in the security of information systems and must not commit any violation of the law related to computer-related offenses.

6.16 The Company does not allow users to install, modify, change the programs on the Company's computers, unless consulted or advised by a system administrator or authorized by the organization's highest authority.

6.17 The Company routes network connections for internet access through the security system by the Company's computers before connecting the network. An anti-virus program must be installed, and a defect of the operating system must be fixed before using the internet system. After finishing the internet use, users must close the web browser to prevent access by others.

6.18 Users are required to access the data resources on the basis of the rights granted by their responsibilities for the performance of the system, networks, and security of the Company. User are prohibited from revealing important confidential information of the Company, except when it is in accordance with the Company's official disclosure regulation. This includes checking the accuracy and reliability of computer information on the internet before using it.

6.19 Users must use the internet system in a manner that does not infringe upon other persons and must not cause damage to the Company as well as not committing any act that is considered an offense under the Computer Crime Act or any relevant laws. In this regard, the use of the internet system to perform their tasks in all cases, users must strictly follow the procedures set forth by the Company.

6.20 The Company arranges the classification of confidentiality by categorizing information according to its mission and prioritization and determines a way to deal with each type of data. Moreover, the Company establishes procedures for managing confidential or sensitive information before cancellation or re-use. In this regard, transmission of important information through the public network must be encoded with an international standard.

6.21 The Company has measures to control the accuracy of information stored, imported, processed, and displayed. In the event that the same data is stored in multiple locations or a collection of related datasets are stored, a control system is required to make information accurate, complete, and consistent. The Company also forms data security measures in case the computer is taken outside the Company's area, such as sending it for repair, or destroying the information stored on the recording media first.

6.22 The Company has control over access to data and data processing equipment by taking into account the use and security in the use of information systems; establishes rules about authorization of access; and assigns the rights so that users at all levels can know, understand, and strictly comply with the established guidelines and realize the importance of maintaining the security of information systems. This is achieved by assigning the rights to use information and information systems, such as the rights to use information system programs and internet usage rights, to users according to their duties and responsibilities. Regarding the rights, the Company must assign, only the rights necessary for the performance of duties and the written approval of the competent authority shall be granted, including reviewing such rights regularly.

6.23 In the event that it is necessary that the users owning the sensitive data have to grant other users access or modify their own information, such as sharing files, the rights must be granted for individual or specific groups only and such permission must be revoked if it is no longer necessary. The data owners must have proof of such authorization and must determine the duration of use and suspend the use immediately after the expiration of such period.

6.24 In case it is necessary to give permission to another person to have the right to use information systems and network systems in an emergency or a temporary case, there must be a procedure or work instruction and approval from the authority must be sought every time. Reasons and necessities must be recorded for such

authorization, including the need to determine the period of use and suspend the use immediately after the expiration of such period.

6.25 The Company has a system to check authentication and users' access rights before entering into the information systems, which is strong enough, such as setting a password that is difficult to guess, and specify that each user has his own account. In this respect, considering whether determination of password is difficult to guess and password usage control is strong or not, the Company uses the following factors for overall consideration:

6.26 Employees

- The password should be long enough. Most international standards recommend a minimum length of 8 characters (Alphabet + Numeric).
- Special characters should be used, for example: :> $ # etc.
- For general users, the password should be changed at least every 2 months. For users with special privileges, such as System Administrators and Default Users, the password should be changed at least every 2 months.
- To change the password each time, a new password should not be repeated to the original for the last 3 times.
- Passwords should not be set in a pattern or easy to guess, such as "abcdef", "Oooooo", "123456" "password" "P@ssword", etc.
- A password should not be set in relation to the user, such as name, surname, date of birth, address, etc.
- A password should not be set with vocabulary in the dictionary.
- The number of times that users are allowed to enter the wrong password should be set. In practice, it is generally 5 times. If the wrong password is entered more than the specified number of times, the system or program will not allow or suspend the use.
- A method for delivering passwords to users should be strong and secure, for example, in a sealed envelope
- Users who have received a password for the first time or a new password should change it immediately.
- Users should keep their password secretly. It should not be written down on paper and attached it to the front of the machine. In case the password is known by another person, the user should change the password immediately.

- In the case of users working together in a manner of shared users licenses, the administrator will send an email to alert the responsible person to change the password to log in to that system when there is a change of user in the agency.

6.27 The Company has a system to check the list of users of important systems on a regular basis and check the list of users who are not authorized to use the system, such as the list of users who have resigned, the list of default users, as well as immediately suspending the use when detected, such as disabling, deleting from the system, or changing password.

6.28 The Company provides the Data Center Room by proportions, for example, dividing the room into network systems, computer servers, back-up power supplies, and batteries for backup power supplies, to facilitate operations and make the accessing control of important computer equipment more efficient.

6.29 The Company makes an agreement for the transfer of information by taking into account the security of information, and the administrator must control such operation to be safe in three aspects, namely confidentiality, data accuracy, and readiness to provide services. The Company requires that the Company and an external entity sign a contract not to disclose the Company's secrets and has measures to monitor and verify the performance and service quality of external service providers to ensure that they are consistent with the contract and agreement.

7. Openness Principle

The Company may disclose personal information of stakeholders, whether as shareholders, employees, business partners, and customers, to individuals or corporate entities as specified below.

7.1 A person or an entity who owns the product (Brand) for the purpose of collecting the history of purchase orders, which the Company will disclose only to the product owner or only personal data that is necessary for the operation.

7.2 Government agencies as the Company must comply with the announcements, rules, and provisions of the law including the Revenue Department, Social Security Office, Department of Business Development, Office of the Consumer Protection Board, Labor Protection and Welfare Office, and Department of Skill Development.

7.3 The Company's partners. The Company may disclose personal information of employees to other parties who have partnership agreements with the Company, such as financial institutions, insurance companies, securities companies, fund management companies for the benefit and welfare of the stakeholders.

7.4 Professional service providers, namely, financial consultants, legal advisors, auditors, internal auditors.

7.5 Service providers for infrastructure and information, data storage, cloud service providers.

7.6 Service providers for marketing, statistical data preparation, advertising, public relations, and communication.

7.7 Any other person required by law, in the event that there are related laws, rules, and regulations, orders of government agencies, regulatory authorities, or an order of a judicial authority requiring the Company to disclose personal information of employees, the Company is obliged to disclose such personal information.

7.8 Assignees and/or duties from the Company, in the event that the Company wishes to transfer its right and duties, including the transfer of some or all of the business, merger, and the change in the shareholding structure of the company, the Company is required to disclose your personal information to the transferees (including potential transferees). In this regard, the transferee's rights and obligations in relation to your personal data will also be in accordance with this policy.

8. Individual Participation Principle

In addition to the fundamental rights of stakeholders in the Company's business operations as the owners of personal data that the Company collects, uses, or discloses personal data including the right to be informed, the right to access information, the right to correct information, the right to request deletion, the right to restrict the provision of information, the right to receive notifications relating to rights, the right of data transfer, the right to refuse the permission of information usage, the right to not allow the use of automated decision-making system, the personal data owners also have specific rights provided by law including:

8.1 Granting consent: You have the right to choose to provide any personal information requested by the Company and agree to the Company to collect, use, or disclose such personal information. However, you must acknowledge that providing incomplete personal information as requested by the Company or not giving consent to the collection, use, or disclosure of such personal information may cause you to restrict your right to use certain services of the Company or result in the Company being unable to provide services to you at if such information is necessary for the Company to provide services to you.

8.2 Accessing and requesting a copy of the personal data or requesting the Company to send the personal data to the data owners itself or other personal data controllers (if such information is in a form that can do so). You can also ask the Company to disclose the acquisition of your personal information if such information is the one that you do not consent to the data storage.

8.3 Objection: You have the right to object to the collection, use, and disclosure of personal data about you. If that information is collected by the Company without your consent or that information is collected, used, or disclosed for direct marketing or research studies.

8.4 Deleting, destroying, or suspending the use: You have the right to request the Company to delete, destroy, or suspend the use of your personal data stored by the Company or to make the information such that it cannot be used to identify the data owner if you revoke or object to the collection, use, disclosure of personal information about you, or when there is no need to store, use, or disclose it for the purposes you have given your consent, or when the Company fails to comply with the law related to the personal data protection.

8.5 Correction: You have the right to request the Company to amend your personal data stored by the Company to be accurate, up-to-date, complete and not cause misunderstanding.

8.6 Withdrawal of consent: You have the right to withdraw your consent to the collection, use, and disclosure of your personal information. However, the withdrawal of your consent will not affect the collection, use, or disclosure of personal information you have previously given consent. In this regard, the said withdrawal may prevent the Company from continuing to provide services to you.

For exercising your rights, you acknowledge that your rights as the owner of personal data mentioned in Articles 8.1 to 8.6 above are the rights that are limited under applicable law, and the Company may refuse your exercise of rights if the Company has legitimate grounds for refusing to exercise such rights.

However, the exercise of rights as the personal data owner as stated in this document would be limited only providing basic services that do not incur unnecessary costs to the personal data controller. If the exercise of the rights of the personal data owner by the person concerned causes damage, fees, expenses for processing the request of the personal data owner, the owner must be liable to reimburse the processing costs for the said exercise of rights.

9. Accountability Principle

9.1 The period of time the Company stores your personal data

Apart from being specified as required by law, the Company will store personal data of stakeholders in its business operations for a period of 10 years from the date that stakeholders have terminated their legal relationship with the Company, unless in cases of necessity related to the use or refutation of legal claims, execution, placement of property, or as specifically required by law.

9.2 Detection system of deletion and destruction of personal data after the expiration of storage period

The Company has in place a detection system to delete or destroy the personal information of stakeholders after the expiration of the storage period, or not involved or more than necessary for the purpose, or as requested by the owner of the personal data, or request to withdraw consent. Unless it is the case that the Company has to keep it for the purpose of freedom of expression, or in accordance with the exceptions of specific laws, including the use that generates the right of legal claims, or compliance with the exercise of legal claims, or raising the defense of legal claims, or for legal compliance.

9.3 Information about the Company as a personal data controller

If you wish to contact the Company to exercise rights regarding personal data, or if you have any other questions about personal data, you can contact the Company at the following details.

Data Controller

Euroasia Total Logistics Public Company Limited

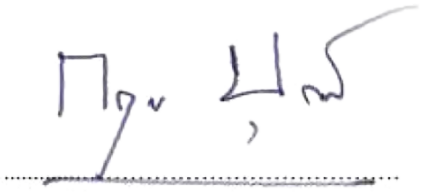
19, 21, Motorway Road, Klongsongtonnoon, Lat Krabang, Bangkok 10520

Telephone: (662) 123 1727

E-mail address: krishavan@etlgps.com

This Privacy Policy was considered and approved by the Board of Directors at the Board of Directors' meeting No. 3/2022 on August 5, 2022. It shall be effective from August 6, 2022 onwards.

Note: This English translation is for reference purposes only. In the event of any discrepancy between the Thai original Privacy Policy and this English translation, the Thai original shall prevail.



Mr. Krishna Boonyachai

Chairman of Board of Directors

Euroasia Total Logistics Public Company Limited