PERSONAL DATA PROTECTION POLICY OF

OMIDA GROUP

WITHIN THE SCOPE OF THE INTERNATIONAL AND DOMESTIC FORWARDING, LOGISTICS, TRANSPORT, CUSTOMS AGENCIES AND OTHER SERVICES RELATED TO COMMODITY TURNOVER

Table of Contents

1. INTRODUCTION AND SCOPE

This document specifies the obligations of the Parties regarding data protection with respect to the process of managing the international and domestic forwarding, logistics, transport, customs agencies and other services related to commodity turnover (hereinafter called: "**Services**").

The policy applies to the Omida Group, which, in accordance with art. 4 pts 19 GDPR is a "group of enterprises", where the companies in the co-administration model are:

- **Omida Spółka Akcyjna, Aleja Grunwaldzka 472C, 80-309 Gdańsk;**
- **Omida Logistics Sp. z o.o., Aleja Grunwaldzka 472C, 80-309 Gdańsk;**
- **Omida Solutions Sp. z o.o., Aleja Grunwaldzka 472C, 80-309 Gdańsk;**
- **NewLogis Sp. z o.o., Aleja Grunwaldzka 472C, 80-309 Gdańsk;**
- **Omida Shared Service Center Sp. z o.o., Aleja Grunwaldzka 472C, 80-309 Gdańsk;**
- **OMIDA IBERICA, S.L. con NIF: B10528941 y con domicilio en calle 60, núm. 25, puerta 5, 08040 Barcelona;**
- **Omida Logistcs S.R.L. Adresa: Str. Col Stefan Stoika, 29, Bl:19, Sc:b, Et:1, Ap:63, 12243 CIF: 46213732 Reg.com.: J40/10227/2022.**

Omida Spółka Akcyjna, as the leading company, controls the processes of personal data processing, identifies the risks of personal data processing and sets security standards accordingly, ensuring adequate protection for all personal data processed in the Omida Group.

Omida Group providing Services to Customers shall act as the data processor entity (hereinafter called: "**Processor**" and the Customer shall act as the **Controller.**

In addition, entities from the Omida Group may also act as separate Data Administrators when they entrust the Service to their Subcontractors who will act as the Processor.

This statement applies to all activities related to the scope of Service, in which the Employees of the Processor or the Subcontractors engaged by the Processor shall be involved in the performance of the personal data process (hereinafter called: "**Data**") by the Controller.

In case of any discrepancies between the mandatory provisions of the European Standard Contractual Clauses (SCC) and the principles of this Data Protection Policy and its constituent documents, the provisions of the European Standard Contractual Clauses (SCC) shall prevail. In case of any other discrepancies between the documents, regulations of this Data Protection Policy shall prevail.

This Data Protection Policy applies to all activities in which persons involved in the performance of duties for or on behalf of the Processor interact with the Controller's personal data.

This Data Protection Policy applies worldwide to all Services provided by Omida to its Customers.

Omida Group reserves the right to amend the principles of this Data Protection Policy without obtaining prior consent or informing its Customers in advance.

2. DEFINITIONS

#	Phrase	Definition
1	**Customer**	means the Party of the Service with Omida Group.
2	**RODO**	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC (General Data Protection Regulation), Journal Of UE L No. 119 of 2016.
3	**Audit reports**	mean current certificates, reports or parts of reports prepared by independent entities (e.g. statutory auditors, internal auditors, data protection inspectors, IT security department, data protection auditors, quality auditors) or

		certification validated by the Controller on the basis of a security or data protection audit.
4	**Data processing**	means an operation or set of operations performed on personal data or sets of personal data in an automated or non-automated manner, such as collecting, recording, organizing, ordering, storing, adapting or modifying, downloading, viewing, using, disclosing by sending, distributing or otherwise sharing , adapting or combining, limiting, deleting or destroying.
5	**Data**	means the Personal Data as specified in Annex No. 1, which are processed by the Processor on behalf of the Controller.
6	**Instruction**	means an instruction in written or oral form, given to the Processor by the Controller, obliging the Processor to perform a specific action as regards the personal data (such as pseudonymisation, blocking access, deletion, data sharing).
7	**Personal data**	means any item of personal or factual information relating to an identified or identifiable natural person.
8	**Processing on behalf**	means the processing of personal data on behalf of the Controller, including storing, modifying, sending, blocking access and deleting personal data by the Processor.
11	**Technical and organisational security measures**	mean measures aimed at protecting personal data against accidental or unlawful destruction, loss, modification, unauthorized disclosure or access, in particular when the processing involves the transmission of data via network, and to protect personal data against any other unlawful form of processing. The above measures include, i.a, pseudonymization and encryption of personal data, the capacity for an continuous ensurance of confidentiality, integrity, availability and resilience of processing systems and services, the capacity to restore the availability of personal data and its access in case of a technical incident, and to periodic reviews, measurement and evaluation the effectiveness of technical and organizational measures to ensure security of processing.

3. SUBJECT MATTER, PURPOSE, DURATION AND SCOPE OF DATA PROCESSING

Subject matter and duration of the Data Processing correspond with the specifications of the Agreement concluded between the Parties.

Scope, type, and purpose of the Personal Data as well as the types of Data and data subjects involved are described detailed in Annex No. 1, which constitutes an integral part of this Data Protection Policy. The Processor shall collect, process and apply the Data solely for the purposes as defined in Annex No. 1.

4. CONTROLLER'S RIGHT TO RENDER INSTRUCTIONS

The Processor shall process the Data solely in accordance with the contractual provisions of the Service and this Data Protection Policy as well as according to the Instructions rendered by the Controller, unless a legal obligation of data processing occurs. Within the framework of the Services, the Controller reserves a comprehensive decisional authority on the nature, scope and methods of data processing, which might be substantiated by him through individual Instructions. Changes regarding the purposes and the procedure have to be agreed between the Parties and to be evidenced. The Processor is solely entitled to grant information to third parties or to data subjects after prior written consent of the Controller.

The instructions of the Controller shall be produced in written form, including electronic mail. In exceptional cases, Instructions may be given orally by the Controller. Such oral Instructions shall be confirmed by a person authorized by the Controller in writing or via e-mail (in text form).

Shall the Processor determine that any Instruction may breach the applicable data protection provisions, he is obliged to notify the Controller forthwith. In case of conspicious breach, the Processor may suspend the execution of the Instruction. Furthermore, the Processor shall be entitled to suspend the execution of the Instruction until its lawfulness is confirmed by a person authorized by the Controller or the Instruction is amended in writing.

5. OBLIGATIONS OF THE CONTROLLER

The Processor shall implement the technical and organizational measures as specified in Annex No. 2 to protect the Data against accidental or unlawful destruction, loss, alteration, modification, unauthorized disclosure, use or access and against all other unlawful forms of processing.

The technical and organizational measures may be adjusted corresponding to a technical and organizational enhancement. Substantial adjustments have to be documented and disclosed to the Controller in writing and are subject to sign-off by the Controller. However, the security level of the adjusted measures may not fall below the originally determined measures level. The Processor shall evidence substantial adjustments and notify the Controller in writing or via e-mail. The Processor shall protect the telecommunication infrastructure against malware (antivirus, firewall). The operating system and other software of IT systems shall be updated and enhanced forthwith.

Shall the Processor perform maintenance works that may lead to significant derogations in the processing of the Controller's personal data with reference to the main Service (e.g. migration into a new system), the Processor notifies the Controller in advance of the intended works in an relevant approach.

The Processor shall conduct periodic audits of internal processes as well as technical and organizational measures to ensure the compliance of data processing as part of his obligations with the requirements of the law on the protection of personal data, and further he shall ensure the protection of the rights of data subjects.

The Processor shall provide the Controller with support in arranging and outlining the updated register of processing activities as well as evaluating the required scope of data protection and prior consultations. At the request of the Controller, he shall be forthwith provided with the required information and documents.

6. SUBCONTRACTING OF THE PERSONAL DATA PROCESSING

Within the meaning of this Data Protection Policy, a Subcontractor constitutes an entity that provides services directly related to the main Service. This does not apply to additional services, such as telecommunications, postal and transport services, maintenance, user service, management of data carriers and other hardware and software resources. However, in the above-mentioned cases, the Processor is obliged under the agreement to ensure data protection and security and to apply appropriate control measures.

Shall during the term of the Service a necessity occur to engage a Subcontractor, the Administrator grants a prior consent. Further / other Subcontractors should effectuate the same data protection requirements as agreed with the Processor. The Processor should notify the Controller in writing (or via e-mail) before placing the order.

The obligations of the Processor and the Subcontractor must be clearly separated. If several Subcontractors are involved, the above also applies to the obligations of individual Subcontractors.

The Controller is entitled to demand an inquiry regarding the content of essential data protection obligations and their performance as part of contractual relations between the Processor and the Subcontractor, if necessary by providing the Controller with relevant contractual documents, and is further entitled to obtain a written response to such inquiry.

If the law stipulates so, the Processor shall conclude additional agreements (including those containing Standard Contractual Clauses approved by the European Commission).

Further, the Processor shall protect the Controller's rights as specified in the above documents, also in relation to Subcontractors, including in particular the Controller's right to issue Instructions and conduct audits.

7. SUPERVISION AND AUDIT RIGHTS

The Controller is entitled, but not obliged, to perform twice a year an audit to verify if the Processor complies with data protection obligations in any location (e.g. inspection of the application of agreed technical and organizational measures) as well as obligations relating to data security and IT security. Further, the Controller is entitled to conduct an inspection at any time for a valid reason (i.e. if there is a reasonable suspicion that the Processor has breached its data protection obligations or obligations regarding data security and IT security). Data protection inspections may further be conducted prior to data processing and after the data processing has been completed. At the request of the Controller, the Processor shall provide him with support for the production of present audit reports.

The Controller may commission the execution of the above-mentioned audit to the Employees (in particular employees responsible for data protection and/or information security) and external auditors authorized by the Controller. Persons engaged by the Controller for the conduct of the audit (hereinafter called: "Auditors") must be obliged to maintain confidentiality in accordance with the provisions of this Data Processing Policy. As provision to achieve protection of the Processor's business secrecy and to avoid breach of the Processor's confidentiality obligation towards third parties during the audit, the Auditors shall be contractually obliged by the Processor not to disclose to the Controller information that the Processor has indicated as confidential information of third parties. With regards to information indicated as confidential information of third parties, the Auditors are obliged to respond solely to general questions of the Controller, for the purpose of compliance with the agreements concluded by the Parties.

The Controller shall notify the Processor in advance, but not later than 14 days in advance, about the date and scope of the intended audit and the appointed Auditors. In the case of an inspection for valid reasons, notification of the inspection may also be submitted less than 14 days before the date of the intended inspection.

For the purposes of aforementioned audit, the Auditors may inspect, during the Processor's regular working hours, the locations where the controlled data and documents are processed or stored, or where certain services are provided.

The Processor shall allow the persons conducting the inspection an unlimited access to the equipment and IT systems necessary to perform the inspection (e.g. computing center rooms, rooms with IT infrastructure and data carriers) and shall disclose all information relevant to the inspection in an orderly, accessible and complete form. The Processor shall provide the Auditors with access to relevantly qualified persons to support the Auditors in conducting the audit. The Processor shall allow the Auditors to produce copies of data and documents relevant to the inspection and submit them to the Auditors. At the request of the Auditor, the Processor shall send copies of such documents and data to the Auditors.

In exceptional cases, the Processor may refuse to consent to the inspection announced by the Controller, if the inspection would constitute an unjustified distortion of the Processor's operations, and the Processor shall notify Controller's Auditors about a further date of the inspection.

The Controller performs the inspection at his own expense. The Administrator is entitled to request the Processor to reimburse such expenses if the audit demonstrates that the Processor or its Subcontractor has materially violated the Data Protection Policy or applicable provisions of law.

8. NOTIFICATION IN CASE OF DATA VIOLATION BY THE PROCESSOR

The Processor shall forthwith inform the Controller (at the latest within 36 hours) about any infringements or suspected infringements caused by him, his Employees or any third party against provisions regarding the Data Processing or against provisions stipulated in the Service. In such case, the Data Protection Officer of the Controller needs to be informed. When necessary, the Controller shall provide documentation standards for the reporting.

The Parties shall grant assistance to each other in elimination of malfunctions or irregularities as regards to the provision of the Services. If any malfunctions or irregularities occur during the Data Processing, the Processor shall immediately investigate the underlying cause and take any measures necessary for the correction of the defects, assuring that such irregularities shall not occur again. The Processor shall inform the Controller immediately and on a regular basis about the status

of the measures until the removal of the malfunction.

In compliance with the binding provisions of law, the Parties may:

- be obliged to provide the competent data protection supervisory authority with the required information pursuant to a written Instruction issued by the Controller or as far as required by the law;
- be obliged to allow a supervisory authority or other authorities (for example, but not limited to investigation authorities) to conduct audits or public inspections to the same extent as such audits may be performed at the Controller's or Processor's premises.

In aforementioned cases:

- The Parties shall support each other regarding such audits, provided that such inspections relate to the data processing activities of the Processor under this Data Protection Policy; and
- The Processor shall inform the Controller forthwith about audits and measures of the data protection supervisory authorities or other above-mentioned authorities, as far as permitted by applicable law.

9. RIGHTS OF THE DATA SUBJECTS

If the Controller is obliged to provide to the data subjects access to information about the storing, using or other processing of personal data of the data subjects (as set out in Art. 15-22 of the RODO), the Processor shall provide the above. If a data subject contacts Processor regarding his rights under applicable law, the Processor shall notify the Controller.

The Processor may not correct, delete or block the Data, unless the Controller issues a corresponding Instruction.

10. DATA CONFIDENTIALITY

The Processor is obliged to safeguard data confidentiality according to applicable data protection laws.

The Processor may only entrust Employees who are committed to data confidentiality with the processing and use of Data. In particular, the Processor shall thoroughly arrange for all persons who are entrusted with the fulfillment of this Data Protection Policy to be carefully selected, to observe the legal provisions regarding data protection and not to transfer information received from the Controller to third parties or otherwise dispose it without authorization. Upon the Controller's request, the Processor shall present relevant evidence for observing these obligations.

11. OBLIGATIONS TO RETURN AND DELETE THE DATA

The Processor is obliged to submit to the Controller any Data, original data storage media (if applicable), respective documents that were provided to him by the Controller for providing the Services immediately after fulfilling the contractual obligations of the Service (at the latest within 30 days). This includes further documents in the possession of the Processor during the execution of the Services including, test facilities (if applicable).

Furthermore, the Processor is obliged to physically delete personal data under the provisions of the Service or consistent with the binding provisions of law on data protection.

The above provisions do not affect the statutory obligation of the Processor regarding the obligation of data storage.

12. LIABILITY

The Controller and the Processor are jointly and severally liable for claims for damages by persons as a result of incorrect data processing as part of the contractual relationship.

Shall the data of such a person be processed, the Processor is held liable to substantiate that the damage was not caused for reasons attributable to him, otherwise, the Processor, upon the first

request, shall release the Controller from any claims made against the Controller as to the entrusted data processing.

The Processor is held liable to the Controller for any damages caused by the Processor, its Employees or Subcontractors engaged by the Processor with regards to the performance of the ordered services.

The above does not apply if the damage was produced as a result of the correct performance of the ordered service or the Instructions issued by the Controller.

13. FINAL PROVISIONS

Separate remuneration for the services is not provided under this Data Protection Policy. The full payment for these services is set out in the Service.

14. ANNEX No. 1 – Data, Purposes, Data Subject

The Processor processes the following data:

- **Type of data:**

- first name and surname;
- residence address;
- seat of the company / business activity;
- telephone number;
- e-mail address;
- nationality;
- PESEL number (national identification *number*);
- ID number;
- NIP number (tax identification number);
- passport number;
- bank account number;
- position title;
- location data.

- **Purposes:** Data is processed and applied solely pursuant to the purposes as stated in teh Service.
- **Data Subjects:** Customers and its Employees.

15. ANNEX No. 2 – Technical and Organisational Measures

Technical and organisational measures, to the implementation of which the Processor is obliged pursuant to the provisions this Data Protection Policy, should include the present state of technical knowledge, implementation costs as well as the nature, scope, circumstances and purposes of processing as well as the probability and degree of threats to the rights and freedom of persons. The above indicated technical and organisational measures that the Processor is obliged to implement pursuant to the provisions this Data Processing Policy include in particular:

- **Risk analysis**

The Processor has analysed the risks related with the particular processing, i.a. the risks related to deletion, breach, manipulation and/or unauthorized access and/or transmission.

- **Risk assessment**

Subject of the assessment should be the risks related to the intended processing (probability, degree, prospects, aspects, legal consequences, etc.). The analysis and assessment should be evidenced, e.g. within the concept of data protection and information security / IT security.

- **Technical and Organisational Measures**

The indicated technical and organisational measures that the Processor is obliged to implement pursuant to the provisions this Data Processing Policy include in particular:

Technical and Organisational Measures		
Confidentiality	Access Control (buildings and premises)	Access to offices solely for authorized persons or in their company
		Door security (electric door opener, security locks, entry card)
		An Employee is constantly present at the reception desk during visiting hours
		Security zones: servers for data processing devices are located in separate rooms, separate from the usual office rooms and a separate access protection system
		Security services outside visiting hours
		Video surveillance at the building entrances
		Alarm system
	Access Control (IT systems and applications)	Authorization by username and password
		Requirements for the complexity of passwords, job locks, users can protect the session with a password screensaver
		Individual and person-related login of the user when logging into the company's network
		Application of firewalls
		Application of Endpoint Protection solutions [extended anti-virus software]
		Application of VPN technology

		Central supervision of authorisations [AD]
	Access Control (data and information)	Physical removal of data from data carriers prior to their disposal
		Service of certified file and data destruction service providers
		Central concept of authorizations [granting rights according to the principle of minimization, granting and using administrator rights limited to the necessary minimum, verification of access rights, separate granting of rights (organizational) and their assignation (technical)]
		Diversification and task-related permissions, profiles, and roles
		User rights management by system administrators
		Password guidelines defining their length and change
	Separation	Technical separation of production and test systems
		Authorization concept in order to separate production and design systems
		Separate databases
		Separate folder and directory structures
		Separate data storage with the concept of rights and roles in the context of commissioned data processing
Integrity	Transfer Control	Secured WLAN network
		Tunneled data connection using VPN technology
		Communication via e-mail through encryption
		Careful selection of service providers [e.g. in the field of destruction of files and data carriers]
Availability and resilience	Availability Control	Fire alarm system
		Backup concept [daily, weekly, monthly]
		Antivirus / firewall protection concept
	Recovery Capability	Regular hardware check [life cycle, performance]
		Incident response management
		Database backup
		Verification of the possibility of recovery
Procedures for periodic review, validation and evaluation	Data Protection Management	Authorisation concept
		Backup concept
		Data recovery concept
		Incident response management
		Personal Data Protection Policy
	Periodic reviews and possible optimization	Periodic audits conducted by the Data Protection Oficer
		Updated register of performed actions

	Data protection by design and data protection by default	Approved procedure