DATA PROCESSING AGREEMENT

This Data Processing Agreement (the "**DPA**") is an integral part of the Terms and details the processing of personal data by Innoship (hereinafter the "**Processor**"), in the name and on behalf of the Customer (hereinafter the "**Controller**").

The capitalized terms not defined in this DPA have the meaning set forth in the Terms.

1. DEFINITIONS

"**Personal Data**" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"**Personal Data of the Controller**" or any other similar expressions, means any Personal Data which the Controller makes available to the Processor for the purpose of fulfilling the Terms, as well as any other Personal Data owned by the Controller, to which the Processor has or gains access for the purpose of performing its obligations under the Terms, detailed according to Annex 2;

"**GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council 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);

"**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;

"**Technical and organizational measures**" means the measures aimed at protecting Personal Data stored, as well as those transmitted within the internal network or to third parties, such as encryption, pseudonymization, firewall, antivirus, etc.

"**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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available in any way, alignment or combination, restriction, erasure or destruction;

"**Services**" means the services provided by the Processor to the Controller which imply processing of Personal Data, as described in the Terms.

2. PROCESSING OF PERSONAL DATA

1. The obligations provided in the Terms and the provision of the Services imply the processing of Personal Data by the Processor. In this respect, the Processor shall observe all applicable legal provisions with respect to the protection of personal data.

2. The Processor, in its capacity as processor, will process the Personal Data of the Controller exclusively for the purpose of providing the Services to the Controller. In this respect, the Processor will only act within the limits provided by the Terms and this DPA, as well as any other further documented instructions given by the Controller.

3. In case the Processor is obliged, under national or EU legal provisions, to transfer Personal Data of the Controller to a third country or an international organization, it will notify the Controller of such aspects before commencing any such processing activities, except if such notification is prohibited by law.

4. The Processor shall promptly inform the Controller if, in its opinion, an instruction received from the Controller infringes the applicable provisions with respect to the protection of personal data.

5. The Processor will answer to all information and/or document requests received from the Controller, for the purpose of verifying compliance with the legal obligations of the Processor with respect to the protection of Personal Data. Moreover, the Processor will allow and contribute to audits performed by the Controller, for this purpose, provided that such audits are not too burdensome or imply disproportionate or unreasonable efforts to be made by the Processor. If the Controller does not find any breach of the data protection legal provisions, it will reimburse the Processor for any reasonable costs incurred with respect to the audit performed by the Controller.

6. The Processor shall create and maintain a record of processing activities performed under this DPA and will provide to the Controller or to any of its designated auditor or proxy, on request, all information included in the record which are necessary for demonstrating compliance with this DPA.

7. If requested, the Processor shall assist the Controller in conducting a data protection impact assessment, by also taking into account the nature of processing and the information available to the Processor.

3. TECHNICAL AND ORGANIZATIONAL MEASURES

1. The Processor will obtain and maintain all necessary licenses, authorizations or approvals, as required by the applicable law, in order to process Personal Data, as well as any data or information derived thereof.

2. The Processor undertakes to implement and to maintain all Technical and organizational measures provided in Annex 1 to this DPA, for the entire duration of this DPA and subsequently, until the erasure or destruction of the Personal Data of the Controller, in accordance with art. 6.3.

3. The Processor will notify the Controller with respect to any Personal Data Breach, within 48 hours from the moment that it gained knowledge of such incident. Moreover, the Processor shall inform the Controller, where possible, with respect to the nature of the breach, volume of data and approximate number of affected persons, as well as the measures taken or proposed to be taken to address or mitigate the adverse effects of the breach.

4. DATA SUBJECT RIGHTS

1. The Processor, taking into account the nature of processing and insofar as this is possible, shall assist the Controller in addressing any complaints or requests from the data subjects, with respect to processing of their personal data, in accordance with the data subjects' rights laid down in Chapter III of the GDPR.

2. In this respect, the Processor will inform the Controller with respect to any complaint or request received from the data subjects, within 7 days from when such complaint or request was received, and will provide any information or documents relevant for this purpose.

5. SUBCONTRACTING

1. The Processor has a general authorization to engage another processor for the purpose of providing the Services, without the prior written authorization of the Controller. However, the Processor shall inform the Controller of any intended changes regarding the processors of the Processor, thereby giving the controller the opportunity to object to such changes.

2. In case the Processor intends to subcontract the provision of the Services to another processor, the Controller may not discretionarily object to such subcontracting of the Services, unless there is a manifestly breach of the applicable legal provisions.

3. In case the Processor is authorized to subcontract the rendering of the Services or of a part thereof, it will conclude a binding agreement with a processor, which will include obligations at least as restrictive as those imposed to the Processor by the Controller.

6. CONFIDENTIALITY OF PERSONAL DATA

1. The confidentiality obligations provided in the Terms will apply accordingly with respect to the Personal Data of the Controller.

2. The Processor shall ensure that all persons which have the duty to process the Personal Data of the Controller will fulfill the following cumulative conditions:

1. are in a contractual relationship with the Processor by which an adequate liability mechanism is ensured;

2. have concluded confidentiality agreements or are under a professional or statutory confidentiality obligation, as the case may be;

3. are informed with respect to the confidential nature of the Personal Data of the Controller and are aware of the Processor's obligations arising from this DPA and the Terms with respect to the Personal Data of the Controller;

3. At the termination of this DPA, for any reasons, the Processor, at the choice of the Controller, will delete or return the Personal Data of the Controller, including any backup copies thereof, except if such further storage is required by the applicable legal provisions. The Processor will sign and provide to the Controller a written statement acknowledging the observance of all requirements related to the deletion and/or returning of the Personal Data of the Controller.

7. TERMINATION

1. This DPA will be automatically terminated at the termination of the Terms.

2. However, any obligations of the Processor under this DPA, which by their nature survive the termination of the DPA, shall continue in full force and effect even after its termination.

8. FINAL PROVISIONS

1. In case of any inconsistencies between the provisions of this DPA any other agreements concluded by the Parties, including without limitation the Terms, the provisions of this DPA will prevail with respect to the obligations of the Parties related to protection of Personal Data.

2. This DPA and the disputes that may arise from its conclusion, execution, interpretation or termination shall be governed by the laws of Romania.

3. In case of a dispute, claim or the like arising under this DPA, the Parties shall attempt to reach an amicable settlement. If an amicable settlement cannot be reached, the dispute shall be submitted to and resolved by the competent Romanian court.

4. This DPA does not imply the payment of an additional remuneration by any of the Parties and it does not derogate from the Terms as regards the financial conditions established by the Parties.

5. If any provision of this DPA is or becomes invalid, illegal or unenforceable, the rest of the DPA will remain in full force and effect. If any provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable, provided that this does not trigger a material adverse change to the initial commercial understanding of the Parties under the Agreement. Otherwise, the Parties shall

make all efforts and negotiate in good faith so as to replace the invalid, illegal or unenforceable provision with a valid, legal and enforceable provision that achieves, to the greatest extent possible, the commercial effects of the original provision.

6. This DPA, together with its annexes, as well as the Terms, if they refer to any aspect which implies processing of Personal Data, represent the full and only agreement of the Parties regarding the processing of Personal Data of the Controller for the purpose of providing the Services, and may only be amended by a written agreement of both Parties.

7. The Parties hereby declare and agree that this Agreement was presented to each Party, that it has been carefully and in detail analyzed and assessed by each Party and that they have been assisted, during every stage of drafting, negotiation and execution, by qualified consultants and advisors (at least from a legal, technical and tax perspective).

8. The Parties hereby declare and agree that this DPA is not a standard form (adhesion) agreement and that it does not contain any standard or unusual clauses, as these are defined under the Romanian law and the DPA has been subject to specific “clause by clause” negotiation and approval of the Parties. Each Party agrees and accepts, irrevocably from the signing of the DPA, all clauses, especially (but without any limitation to) the following Articles 2.2, 2.3, 2.6, 3, 5.3, 6.2, 8.2, 8.3, 8.4.

ANNEX 1 – Technical and organizational measures

1. Security of Personal Data

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk for the Personal Data of the Controller, including as appropriate:

    1. Pseudonymization and encryption;

    2. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

    3. The ability to restore the availability and access to Personal Data of the Controller in a timely manner in the event of a physical or technical incident;

    4. A process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;

    5. A backup and restore procedure for Personal Data;

    6. Implementation of an access control system applicable to all users which have access to the IT system of the Processor;

    7. Use of authentication credentials;

    8. Traffic to and from the IT system is monitored and controlled by firewall and antivirus applications, or other unauthorized access detection systems, which are appropriately configured and regularly updated, in accordance with the updates available from the developer;

    9. User may not disable or bypass the security settings, nor can they install or deactivate unauthorized software applications.

2. In assessing the appropriate level of security, the Processor shall take into account all the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

2. Physical security

1. Any rooms and areas in which physical elements or components of the IT infrastructure are located or terminals which allow any access, are restricted to unauthorized personnel. Adequate technical measures (*e.g.*, systems for detection and alerting of unauthorized access, card access gates and access point blocking systems) or organizational measures (*e.g.*, security agents) will be implemented, for the purpose of preventing any unauthorized personnel to access such areas and/or access points.

3. Human resources management

1. The Processor shall ensure that all its employees understand their duties and obligations with respect to the processing of Personal Data.

4. Policies and procedures

1. The Processor has implemented internal policies and procedures with respect to processing of Personal Data.

5. Personal Data Breach

1. The Processor ensures that it has implemented appropriate technical measures for the detection of a Personal Data Breach and that it has implemented a Personal Data Breach response policy, which ensures an effective response to any incidents related to Personal Data.

ANNEX 2 – Personal Data of the Controller

Category of Data Subjects

- Consumers, clients of the Controller;
- Contact persons and/or legal representatives, in case of clients of the Controller which are legal entities.

Types of Personal Data

- Identification data (*first name, surname*);
- Contact data (*delivery address, email address, telephone number*);
- Comments from orders (*if applicable*).

Processing Operations

☒collecting; □registration; □organizing; ☒structuring; ☒storage; □adaptation or modification; □extraction; □consultation; □use; ☒disclosure by transmission, dissemination or placement disposition in any other way; □alignment or combination; □restriction; □deletion or destruction.

Nature and purpose of Processing

Processing operations are performed by automatic means.

Purpose of processing:

- Sending orders, including all personal data related to it, to couriers agreed by the Parties, for delivery;
- Storing data regarding the orders for consultation by the Controller;

Processing Time

Processing will take place during the validity period of the DPA.