Data Protection Agreement

This Data Protection Agreement ("**DPA**") is attached to, and forms part of, <u>Innomotics Inc. Standard Terms and Conditions of Purchase</u> ("**Agreement**"). All terms used but not defined in this DPA will have the same meanings provided in the Agreement. If there is any conflict between any provision in this DPA and any provision in the Agreement, this DPA shall control.

1. Definitions

"**Applicable Data Protection Law**" means all applicable law pertaining to the Processing of Personal Data under the Agreement, including, but not limited to, (i) for Personal Data originating from an Authorized Entity located within the EEA, the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), and (ii) for Personal Data originating from an Authorized Entity located within the UK, the UK GDPR and the UK Data Protection Act 2018.

"**Authorized Entity**" shall mean any entity (including Innomotics and its group companies) acting as Controller and being entitled by the Agreement to directly or indirectly access or use Services.

"**Controller**" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"**Country with an Adequacy Decision**" means any country for which the EU Commission has decided that such country ensures an adequate level of data protection and for personal data originating from the UK, any country for which UK adequacy regulations have been made under sections 17A or 74A of the Data Protection Act 2018.

"**Data Breach**" means any breach of security (i) leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed, or (ii) would require notification of such event to any third party pursuant to applicable law.

"**Data Subject**" means an identified or identifiable natural person; 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.

"**EEA**" means the European Economic Area.

"**EU Standard Contractual Clauses**" means the Standard Contractual Clauses (EU) 2021/914.

"**Innomotics**" means the respective Innomotics group company being a party to the Agreement or related individual agreement, adoption agreement, purchase order or other contractual arrangements referencing the Agreement.

"**Origination Area**" means the EEA the UK, Switzerland and each country with similar adequacy requirements as contained in Art. 45 et seq. GDPR.

"**Personal Data**" means any information relating to an identified or identifiable natural person; 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.

"**Processing**" (and its other forms such as **Process, Processes, Processed**) 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, alignment or combination, restriction, erasure or destruction.

"**Processor**" means a natural or legal person, public authority, agency or any other body which Processes Personal Data on behalf of a Controller.

"**Processor Binding Corporate Rules**" or "**Processor BCR**" means binding corporate rules for processors which are approved by the competent supervisory authority.

"**Provider**" means the provider being a party to the Agreement or related individual agreement, adoption agreement, purchase order or other contractual arrangements referencing the Agreement.

"**Restricted Personal Data**" means any Personal Data originating from an Authorized Entity located within an Origination Area.

"**Restricted Transfer(s)**" means any Processing (including transfers, international access and onward transfers) of Restricted Personal Data by Provider or any of its Subprocessors outside the relevant Origination Area.

"**Services**" shall mean the Services under the Agreement provided by Provider acting in its role as Processor within the meaning of this DPA. In the Agreement, Services as defined herein may be referred to as "Cloud-Services", "Online Services", "Offering", "Product" or otherwise.

"**Standard Contractual Clauses**" means the EU Standard Contractual Clauses; and the UK Standard Contractual Clauses.

"**Subprocessor(s)**" shall mean any further Processor engaged in the performance of the Services.

"**Transfer Safeguard(s)**" shall mean appropriate safeguards for Restricted Transfers as required by Applicable Data Protection Law, such as appropriate safeguards as required by Article 46 GDPR.

"**UK GDPR**" means the GDPR as saved into United Kingdom law by virtue of Section 3 of the United Kingdom's European Union (Withdrawal) Act 2018.

"**UK Standard Contractual Clauses**" means such standard data protection clauses as are adopted from time to time by the UK Information Commissioners Office ("ICO") in accordance with Article 46(2) of the UK GDPR including, but not limited to, the international data transfer agreement (UK IDTA), and the EU Standard Contractual Clauses as amended by ICO's International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ("**UK Addendum**"). (Data Protection and the EU | ICO)

2. Compliance with Applicable Data Protection Law

The parties shall observe Applicable Data Protection Law as they apply to them and as required herein. In providing Services, Provider shall in particular comply with the provisions of Applicable Data Protection Law regarding the Processing of Personal Data as a Processor.

3. Scope of the processing

Provider shall Process Personal Data only (i) in accordance with the terms of this DPA; or (ii) on other documented instructions from Innomotics. Provider shall not Process Personal Data for its own purposes or transfer it to third parties, unless permitted by this DPA. Provider shall immediately inform Innomotics if, in its opinion, an instruction from Innomotics infringes Applicable Data Protection Law.

4. Details of the processing operations provided by provider

The details of the Processing operations provided by Provider - in particular the subject matter of the Processing, the nature and purpose of the Processing, types of Personal Data Processed and the categories of affected Data Subjects - are specified in **Annex I**.

5. Technical and organizational measures

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, Provider shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, but not limited to, as appropriate: (i) the pseudonymisation and encryption of Personal Data; (ii) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; (iii) the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; (iv) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing. Without prejudice to the generality of the preceding sentence, Provider shall at all times implement at least the technical and organizational measures described in **Annex II**.

6. Commitment to confidentiality

Provider shall limit its personnel's access to Personal Data on a need-to-know basis. Provider shall provide detailed notice to its personnel about the applicable statutory and contractual provisions regarding data protection. Provider shall put its personnel under an obligation to comply with such provisions and, in particular, to hold Personal Data secret and not to Process Personal Data other than according to Innomotics' instructions. The obligation to secrecy shall continue to apply after the expiry of this Agreement and the personnel's contractual relationship with the Provider. Provider will provide proof of such obligation upon request.

7. Subprocessors

a) Provider has Innomotics' general authorization for the engagement of Subprocessors. A current list of Subprocessors commissioned by Provider is contained in Annex III.

b) The Provider shall specifically inform Innomotics in writing of any intended changes to that list through the addition or replacement of Subprocessors at least 30 days in advance. Provider shall provide Innomotics with the information necessary to enable Innomotics to exercise the right to object. If Innomotics raises no objections within this 30-day period, then this shall be taken as an approval of the new Subprocessor. If Innomotics raises objections, Provider will - before authorizing the Subprocessor to access Personal Data - use reasonable efforts to address the concerns and reservations expressed by Innomotics and (i) refrain from using the Subprocessor or (ii) propose to Innomotics a reasonable change in the Services or Innomotics' configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Subprocessor. If Provider is unable to eliminate the grounds for the objection by Innomotics, Innomotics is entitled to terminate the affected Services without any damages or penalties. In the event of termination by Innomotics, Provider will refund any prepaid amounts for the applicable Service on a pro-rata basis.

c) Where the Provider engages a Subprocessor to carry out specific processing activities (on behalf of Innomotics and/or Authorized Entities), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the Provider under this DPA.

d) Provider shall provide, at Innomotics' request, a copy of such a Subprocessor contract and any subsequent amendments to Innomotics. To the extent necessary to protect business secrets or other confidential information, including Personal Data, Provider may redact the text of the contract prior to sharing a copy.

e) Provider shall adequately and regularly audit the Subprocessor with respect to compliance with these requirements and document the results of such audits.

f)   Provider shall remain fully responsible to Innomotics for the performance of the Subprocessor's obligations under its contract with the Provider. Provider shall immediately inform Innomotics of any failure by the Subprocessor to fulfil its obligations under that contract.

8. International Data Processing

Provider shall ensure that Restricted Transfers are covered by adequate Transfer Safeguards as set forth in <u>Annexes III and IV</u>, unless the Restricted Transfer is made to a Country with an Adequacy Decision.

9. Provider's assistance

Provider shall reasonably assist Innomotics in ensuring compliance with Applicable Data Protection Law, in particular by assisting Innomotics as follows:

a) Correction, Deletion or Restriction of Processing. Provider shall either (i) provide the ability to rectify, erase or restrict the Processing of Personal Data via the functionalities of the Services, or (ii) rectify, erase or restrict the Processing of Personal Data as instructed by Innomotics.

b) Access to Personal Data. To the extent information relating to a Data Subject is not accessible through the Service, Provider will, as necessary to enable Innomotics and Authorized Entities to meet its obligations under applicable Data Protection Laws, provide assistance to make such information available to Innomotics and/or Authorized Entities.

c) Data Subject and Authority Requests. Provider shall promptly notify Innomotics concerning: (i) any request or complaints received or any notices of investigation by a law enforcement, governmental or regulatory authority or agency; and (ii) any request received directly from any Data Subject about their Personal Data.

With respect to (i) and (ii) above, Provider shall not respond without instructions from Innomotics. If so instructed, Provider shall reasonably support Innomotics in answering such requests.

d)   Data Portability. Upon Innomotics' request and if required under Applicable Data Protection Law, Provider will either (i) provide the ability to extract Personal Data by reference to a specific Data Subject in accordance with the functionalities of the Service or (ii) make the relevant set of data available to Innomotics and/or the respective Authorized Entity, in each case in a structured, commonly used and machine-readable format.

e) Data Protection Impact Assessments. If requested by Innomotics, Provider shall provide all information and reasonable support to carry out data protection impact assessments under Applicable Data Protection Laws.

f) Prior Consultation. If requested by Innomotics, Provider shall assist Innomotics in ensuring compliance with the obligation to consult the competent supervisory authority/ies prior to Processing where a data protection impact assessment indicates that the Processing would result in a high risk in the absence of measures taken by Innomotics to mitigate the risk.

10. Termination of the data Processing relationship

Upon termination of the data Processing relationship, unless otherwise instructed by Innomotics or set forth herein, Provider shall return to Innomotics all Personal Data made available to Provider or obtained or generated by Provider in connection with the contractually agreed Services and shall irrevocably delete or destroy any remaining data. The deletion or destruction shall be confirmed by Provider in writing upon request.

11. Notification obligations

a) Provider shall notify Innomotics immediately but in any event within 48 hours in case Provider discovers or reasonably suspects any Data Breach.

b) In the notification to Innomotics, Provider shall provide Innomotics with the following information: (i) The details of a contact point where more information can be obtained, (ii) a description of the nature of the breach (including, where possible, names, categories and approximate number of Data Subjects and personal data records concerned), (iii) its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

c) Any notifications under this Section 11 shall be made (i) to the respective point of contact identified in the Agreement and (ii) to innomotics.legal-compliance@innomotics.com.

d) Provider shall, at Provider's cost and expense, (i) cooperate fully with Innomotics in the investigation of a Data Breach, (ii) assist and cooperate with Innomotics concerning any legally-required notifications or disclosures to affected persons (by individual communication, public communication via the media or by similar measures), law enforcement, regulators and/or other third parties, and (iii) any other action Innomotics deems necessary regarding such Data Breach and any dispute, inquiry or claim that concerns the Data Breach.

e) Unless applicable law or an order of a competent regulator requires otherwise, Innomotics shall make the ultimate determination, in its sole discretion, (i) whether a Data Breach requires notification and (ii) of the manner of the notification. In the event that the Provider provides such notifications regarding a Data Breach, any such notices must be approved, in advance, by Innomotics.

f) Provider shall at its cost take appropriate measures to address the Data Breach, including measures to mitigate its adverse effects (including steps to protect the operating environment). Provider also shall take prompt steps designed to prevent the recurrence of any Data Breach, including any action required by Applicable Data Protection Law.

g) Provider shall reimburse to Innomotics all costs and expenses incurred for such Data Breach caused by Provider, including but not limited to the costs of providing credit monitoring to the individuals whose Personal Data was affected by the Data Breach. Limitations of liability in favor of Provider under this Agreement shall not apply in this respect.

12. Documentation and Audits

a) Provider shall (i) monitor, by appropriate means, its own compliance with its data protection obligations under this DPA and Applicable Data Protection Law, (ii) create related periodic (at least annual) and occasion-based reports (each a "**Report**") and (iii) make the Reports available to Innomotics and Authorized Entities upon request. Where a control standard and framework implemented by Provider provides for controls, such controls will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.

b) If required to adequately address its audit rights and obligations under Applicable Data Protection Law, the applicable Transfer Safeguards or if requested by a competent data protection authority or other competent government authority or agency, Provider shall make available to Innomotics and Authorized Entities - in addition to the Reports - all further information reasonably requested and allow for and contribute to audits, including inspections, conducted by Innomotics or Authorized Entities or another auditor mandated by Innomotics or Authorized Entities. For such purpose, Innomotics, Authorized Entities or another auditor mandated by Innomotics or Authorized Entities shall also have the right to carry out on-site inspections during regular business hours, without disrupting the Provider's business operations, and if necessary, after a reasonable prior notice.

13. Use of Cookies

If the Service makes use of cookies or similar technologies, the following shall apply: Provider shall, unless specifically agreed otherwise by Innomotics with reference to this Section 13, only store information (e.g., by writing a cookie), or gain access to information already stored in the terminal equipment of a user of the Service (e.g., via a cookie) for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the Provider to provide the provide the core functionalities of the Services.

14. Miscellaneous

Provider understands and agrees that the requirements in this DPA are an integral part of the Agreement and, a material breach of any of these requirements shall be considered a material breach by Provider of the Agreement, entitling Innomotics to material breach related remedies contained in the Agreement.

15. Additional Requirements concerning data of Innomotics US Companies

If and to the extent Provider accesses Personal Data received from an Innomotics group company established in the United States of America ("**Innomotics US Company**") or of a Data Subject that is the resident of the United States of America, then in addition to the above Provider (i) shall comply with U.S federal, state and local laws regarding Personal Data that are applicable to Provider, such Personal Data, and owners or controllers of such Personal Data; when the foregoing is applicable, the term "Applicable Data Protection Law" as used herein shall include the foregoing laws; (ii) except as specifically provided herein or the Agreement, shall not sell, share, rent, release, disclose, disseminate, or make available Personal Data to third parties; and shall not combine the Personal Data with other information; (iii) shall notify Innomotics if Provider makes a determination that Provider can no longer meet its obligations hereunder; (iv) shall ensure that each person processing Personal Data is subject to a duty of confidentiality with respect to the Personal Data; (v) shall be deemed, and shall act as, a "service provider" under Applicable Data Protection Law (including the California Consumer Privacy Act, its implementing regulations, and any amendments thereto), and (vii) hereby certifies that it understands the restrictions contained herein and will comply with them.