MODULE DPAC
DATA PROTECTION AGREEMENT: CONTROLLER

1. DEFINITIONS AND INTERPRETATION

Data Protection Laws means applicable data protection legislation including, but not limited to, the General Data Protection Regulation (Regulation (EU) 2016/679), and local equivalent;

Data Subjects means an identified or identifiable natural person;

Personal Data means any information relating to an identified or identifiable natural person defined under the Data Protection Laws;

Personal Data Incident(s) means a breach of security relating to Personal Data in KINTO's systems or facilities leading to accidental or unlawful destruction, loss, damage and/or alteration of Personal Data; (ii) unauthorised disclosure and/or access of Prersonal Data; and/or (iii) any and all other unauthorised or unlawful forms of Processing upon Personal Data;

Processing, Process and processed means one or more of the following activities: collection; recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure, disseminaton, alignment, restriction, erasure, destruction performed on the Personal Data;

SCC means EU standard Contractual Clauses included in Decision 2021/915;

1.1 If Customer and KINTO enter into SCC in relation to the same subject matter as this module DPAC, SCC shall prevail in the event of any conflict of terms.

2. **Purposes:** KINTO shall process Personal Data as Data Controller as defined under Data Protection Laws and solely for the purposes necessary for the fulfilment of services described under this Agreement and all SOW/Orders placed under the Agreement in a manner consistent with Data Protection Laws.

3. **Authorized Disclosures:** KINTO may disclose Personal Data to subcontractors or service providers only when permitted under Data Protection Laws. In such case, KINTO shall ensure that its subcontractors, service providers acting as Data Processors are contractually bound to no less than the data privacy standards stated in this Agreement. In accordance with applicable Data Protection Laws KINTO shall be responsible for its Data Processors

4. Data Subjects' Rights

Inquiries by Data Subjects in relation to access, rectification and deletion of Personal Data processed by KINTO shall be KINTO's responsibility and shall be responded to within 30 calendar days from receiving the inquiry. KINTO shall ensure its subject access request procedure and up-to-date privacy policy are readily available to such Data Subjects.

5. Data Security

5.1 KINTO shall comply and implement all administrative, technical and organizational measures to ensure at all times the confidentiality, integrity, availability and resilience of KINTO systems, Processes and procedures that involve the Processing of Personal Data.

5.2 KINTO shall protect Personal Data against (i) accidental or unlawful destruction, loss, damage and/or alteration; (ii) unauthorised disclosure and/or access; and/or (iii) any and all other unauthorised or unlawful forms of Processing.

5.3 A list of such measures is set forth in the Security Requirements available at https://legal.kintozero.com/wp-content/uploads/2025/10/TOMIST.pdf?v=1760360028 may be amended from time to time and KINTO shall comply at all times with these measures in providing the data Processing services and performing its obligations under this Agreement.

6. PERSONAL DATA INCIDENT MANAGEMENT PROGRAM

6.1 KINTO will have in place a program to manage the consequences of Personal Data Incidents, defined as breaches of security relating to Personal Data and leading to accidental or unlawful destruction, loss, damage and/or alteration; (ii) unauthorised disclosure and/or access; and/or (iii) any and all other unauthorised or unlawful forms of Processing.

6.2 Upon the occurrence of a Personal Data Incident, KINTO shall promptly inform the Personal Data Incident to Customer via email including a description of the incident. KINTO shall also take prompt steps to contain the Incident and mitigate its consequences; investigate it; assess the risks and potential adverse consequences associated with the Incident; and determine the appropriate response and action, including where relevant, towards the Data Subjects without undue delay.

7. International Data Transfers

7.1 KINTO shall comply with Data Protection Laws in connection with any international transfer of Personal Data.

7.2 Any transfer of Personal Data by Customer to KINTO for the purposes set out above to a country located outside the European Union/European Economic Area not deemed to have adequate protection under Data Protection Laws shall be legitimised through implementation of SCC which is hereby recognised as an approved transfer method comporting with Data Protection Laws. KINTO confirms it has authority to enter into SCC on behalf of itself and its Affiliates and their commitment to adhere to all terms of SCC.

7.3 Any transfer of Personal Data by KINTO to a country located outside the European Union/European Economic Area not deemed to have adequate protection under Data Protection Laws (intra-group or otherwise) shall be legitimised by KINTO through an approved transfer method which comports with Data Protection Laws.

8. Deletion

Upon termination of this Agreement, KINTO will promptly delete any Personal Data and all copies thereof, and in any event no later than the applicable local retention periods as set out by the Data Protection Laws or relevant data protection supervisory authority or regulatory body. KINTO shall provide to Customer, upon Customer's request, written proof of such deletion in a timely manner