Data Processing Addendum - APAC

This Addendum supplements the i2 Licence Agreement and any associated Order Forms or Quotes (together, the "**Agreement**") entered into between N. Harris Computer Corporation, trading as i2 Group, and its Affiliates ("**Supplier**" or "**Service Provider**"), and the entity identified as licensee under the Agreement ("**Customer**").

This Addendum applies whenever the Service Provider Processes Personal Information relating to, or originating from, individuals in the APAC Territory in connection with the Services under the Agreement.

1. DEFINITIONS

1.1 "**APAC Territory**" means any one or more of the following jurisdictions: Australia, the People's Republic of China, Hong Kong, Japan, South Korea, India, Indonesia, Thailand, Vietnam, Malaysia, New Zealand, the Philippines, Singapore, or Taiwan, and includes any jurisdiction in which Personal Information is accessed, stored, or otherwise Processed by the Service Provider.

1.2 "**Customer**" has the meaning given to it in the Agreement or any associated Order Form or Quote, as applicable.

1.3 "**Personal Information**" means any information or opinion, whether true or not and whether recorded in a material form or not, about an identified or reasonably identifiable individual, including information that is protected as "personal information", "personal data" or equivalent under applicable Privacy Regulations.

1.4 "**Privacy Regulations**" means all applicable laws, statutes, ordinances, regulations, rules, codes, directives, circulars, judgments, decisions, decrees, orders, determinations, or binding guidance issued by any governmental or regulatory authority in the APAC Territory, whether currently in force or enacted in the future, that regulate or govern the Processing of Personal Information, including, without limitation:

1.4.1 **Australia**:

Privacy Act 1988 (Cth), including its application to entities exempt as "small business operators" under the Act.

1.4.2 **New Zealand**:

Privacy Act 2020.

1.4.3 **Taiwan**:

Personal Data Protection Act.

1.4.4 **Japan**:

Act on the Protection of Personal Information (Kojin Joho no Hogo ni Kansuru Houritsu, Law No. 57 of 2003), as amended.

1.4.5 **Malaysia**:

Personal Data Protection Act 2010.

1.4.6 **South Korea**:

Personal Information Protection Act (PIPA) 2011.

1.4.7 **People's Republic of China**:

1.4.7.1 Cybersecurity Law of the PRC (2017).

1.4.7.2 Data Security Law (2021).

1.4.7.3 Personal Information Protection Law (2021).

1.4.7.4 Relevant provisions of the Civil Code of the PRC.

1.4.7.5 People's Bank of China Notice (2011) No.17 on the Protection of Personal Financial Information.

1.4.8 **India**:

1.4.8.1 Information Technology Act 2000, including the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

1.4.8.2 Digital Personal Data Protection Act 2023 (to the extent applicable).

1.4.9 **Hong Kong**:

Personal Data (Privacy) Ordinance (Cap. 486, Laws of Hong Kong), as amended, including by the Personal Data (Privacy) (Amendment) Ordinance 2012.

1.4.10 **Philippines**:

Data Privacy Act 2012 and implementing rules and regulations.

1.4.11 **Singapore**:

Personal Data Protection Act 2012, including applicable subsidiary legislation and advisory guidelines.

1.4.12 **Indonesia**:

Personal Data Protection Law (Law No. 27 of 2022).

1.4.13 **Thailand**:

Personal Data Protection Act B.E. 2562 (2019).

1.4.14 **Vietnam**:

Decree No. 13/2023/ND-CP on Personal Data Protection.

1.4.15 Any other equivalent or successor legislation, including regional frameworks or binding interpretations from data protection authorities within the APAC Territory.

1.4.16 For the avoidance of doubt, Privacy Regulations shall include any binding guidance or requirements issued by competent data protection regulators, supervisory authorities, or central banks that have legal force and effect within the relevant jurisdiction(s).

1.5 "**Processing**" (and "**Process**") means any operation or set of operations performed on Personal Information, including collection, access, use, disclosure, recording, storage, alteration, retrieval, alignment, combination, transfer, restriction, erasure, or destruction, whether by automated means or otherwise.

1.6 "**Service Provider**" means Supplier, its Affiliates, employees, agents, and authorised subcontractors engaged in delivering the Services under the Agreement.

1.7 Capitalised terms not defined herein shall have the meanings given to them in the Agreement. In the event of a conflict between this Addendum and the Agreement, this Addendum shall prevail to the extent of such conflict with respect to the Processing of Personal Information.

2. OBLIGATIONS IN RESPECT OF PERSONAL INFORMATION

In Processing Personal Information on behalf of the Customer, the Service Provider shall (and shall procure that its personnel, subcontractors, and agents):

2.1 Comply at all times with applicable Privacy Regulations and provide reasonable cooperation to the Customer in fulfilling its obligations thereunder.

2.2 Process Personal Information only in accordance with the Customer's documented instructions or as necessary to perform the Services. If the Service Provider cannot comply, it shall immediately inform the Customer, who may suspend or terminate Processing.

2.3 Not use, disclose, or modify Personal Information except as permitted under the Agreement or required by applicable law.

2.4 Implement and maintain appropriate technical and organisational measures to protect Personal Information against unauthorised or unlawful Processing and accidental loss, destruction, or damage.

2.5 Ensure access to Personal Information is limited to personnel with a legitimate "need-to-know" and under binding confidentiality obligations.

2.6 Notify the Customer without undue delay (and in any event within 72 hours) of any actual or suspected unauthorised access, disclosure, loss, or breach of Personal Information, and provide reasonable assistance in investigation, notification, and remediation.

2.7 The Service Provider shall document all Personal Information breaches, including the facts relating to the breach, its effects, and the remedial actions taken. This documentation shall be made available to the Customer on request to enable compliance verification.

2.8 Upon termination or expiry of the Agreement, or at the Customer's written request, return or securely delete all Personal Information, unless retention is required by applicable law. Where Personal Information is deleted, the Service Provider shall confirm such deletion in writing.

2.9 Not disclose Personal Information to any third party, including subcontractors, without the Customer's prior written consent and only under written terms equivalent to this Addendum. The Service Provider shall remain fully liable for the acts and omissions of such third parties.

2.10 Not transfer Personal Information outside the jurisdiction in which it was originally collected or otherwise subject to regulation, except in compliance with applicable Privacy Regulations and shall implement appropriate safeguards in accordance with applicable Privacy Regulations, including but not limited to entering into government-approved contractual clauses, maintaining records of transfer impact assessments, and ensuring ongoing compliance monitoring where required by law.

2.11 Provide reasonable assistance to the Customer to respond to data subject rights requests and regulatory inquiries or assessments under applicable Privacy Regulations.

2.12 Notify the Customer without undue delay of:

2.12.1 Any legally binding request for disclosure by a governmental or regulatory authority, unless prohibited by law.

2.12.2 Any data subject request relating to Personal Information received directly by the Service Provider.

2.12.3 Any regulatory investigation or enforcement action concerning the Processing of Personal Information under this Addendum.

2.13 Correct or annotate Personal Information as directed by the Customer, and refrain from making corrections unless instructed.

2.14 Undertake privacy training and awareness measures for its staff, as reasonably required by the Customer.

2.15 Ensure all Processing is traceable and, where applicable, documented to demonstrate compliance with this Addendum.

3. DIRECT COLLECTION BY SERVICE PROVIDER

Where the Service Provider collects Personal Information directly from individuals in connection with the Agreement, it shall:

3.1 Provide all notices required under applicable Privacy Regulations, including informing individuals of the purpose and legal basis for Processing.

3.2 Obtain any required consent for the collection, use, disclosure, and international transfer of Personal Information, ensuring such consent is freely given, specific, informed, and unambiguous.

3.3 Comply with all applicable requirements for individual rights, including access, correction, objection, and deletion under relevant Privacy Regulations.

3.4 Where required by applicable Privacy Regulations, the Service Provider shall maintain a record of the legal basis relied upon for each Processing activity involving direct collection and make this available to the Customer upon request.

4. COMPLIANCE INFORMATION RIGHTS

4.1 The Supplier shall provide to the Customer, its Affiliates, authorised representatives, and regulatory authorities reasonably sufficient information to demonstrate its compliance with the is Addendum and applicable Privacy Regulations. This may include, without limitation, the results of internal audits, test and reviews as well as any external certifications such ISO or SOC certifications.

4.2 If required by a regulatory authority, or applicable Privacy Regulations, the Customer, its Affiliates, authorised representatives, and regulatory authorities ("**Customer Auditors**") may audit the Service Provider's compliance with this Addendum, including through on-site inspections.

4.3 Audits shall be conducted during normal business hours and with reasonable prior written notice. Each party shall bear its own costs.

4.4 The Customer Auditors shall be subject to non-disclosure obligations and shall not have access to the Service Provider's systems or other customer data.

4.5 Where the Service Provider reasonably believes that any Customer instruction in connection with Personal Information would contravene applicable law, it shall notify the Customer without delay.

4.6 The Service Provider shall implement and maintain internal data protection audits or reviews at reasonable intervals and make available summaries of such assessments to the Customer upon written request.

5. LIABILITY AND EQUITABLE RELIEF

5.1 The Service Provider shall fully indemnify and hold harmless the Customer against any losses, liabilities, damages, claims, or fines, arising from a breach of this Addendum or applicable Privacy Regulations.

5.2 The Service Provider acknowledges that breach of this Addendum may cause irreparable harm to the Customer for which damages alone may be inadequate. Accordingly, the Customer shall be entitled to seek immediate injunctive or equitable relief in the event of a breach or threatened breach.

5.3 The limitations or exclusions of liability in the Agreement shall not apply to the Service Provider's liability under this Addendum for:

5.3.1 Unauthorised disclosure of Personal Information.

5.3.2 Regulatory fines incurred due to the Service Provider's breach.

5.3.3 Failure to implement adequate security measures.

6. SURVIVAL

Clauses 2 (Obligations in Respect of Personal Information), 3 (Direct Collection), 4 (Customer's Use), 5 (Audit), and 6 (Liability) shall survive the termination or expiry of this Addendum or the Agreement, for so long as the Service Provider continues to hold or Process Personal Information.

7. GOVERNING LAW AND JURISDICTION

7.1 For disputes or questions arising under this Addendum in connection with Personal Information originating from a specific jurisdiction within the APAC Territory, the Privacy Regulations of the jurisdiction from which such Personal Information originated shall govern the interpretation of data protection obligations under this Addendum.

7.2 Subject to the above, all other disputes shall be governed by the governing law and forum selection provisions in the Agreement. In the event of ambiguity, the parties agree that data protection issues shall be interpreted in favour of compliance with the most protective applicable legal standard.

7.3 In the event of conflicting interpretations between multiple applicable Privacy Regulations, the parties agree to apply the highest standard of protection required under any applicable jurisdiction.