PRODUCT SPECIFIC TERMS – INTENT ONE

1. GENERAL

1.1. These Product Specific Terms supplement the General Terms which apply to this Agreement where the Client subscribes to IntentOne.

1.2. If there are any conflicts between the General Terms and these Product Specific Terms, these Product Specific Terms shall apply, save that the Data Processing Addendum shall prevail over these Product Specific Terms in respect of any data protection matter.

1.3. Unless otherwise stated within these Product Specific Terms, any capitalised terms shall have the same meanings as those in the General Terms.

2. SECURITY

2.1. The Client is solely responsible for implementing and maintaining appropriate security measures, configurations and access controls within the Client Environment (as defined below) to protect IntentOne, associated data and any systems interacting with it. This includes, but is not limited to:

2.1.1. implementing and maintaining firewalls, intrusion detection systems and encryption;

2.1.2. applying security patches and updates to the Client's infrastructure and any third-party software components;

2.1.3. managing user access rights, enforcing multi-factor authentication and ensuring secure credentials management; and

2.1.4. conducting regular security assessments and compliance audits of the Client Environment.

2.2. IHQ shall not be responsible for any unauthorised access, data loss, corruption or security breaches occurring within the Client Environment. For the purposes of these Product Specific Terms, "**Client Environment**" means the systems, networks, devices, applications and user accounts owned or controlled by the Client or its end users, and expressly excludes the hosted IntentOne platform and any systems or infrastructure operated by or on behalf of IHQ. Nothing in these Product Specific Terms limits or excludes IHQ's obligations under Clauses 6 and 7 of the Data Processing Addendum, or under Article 32 of the UK GDPR or the EU GDPR, in respect of the hosted IntentOne platform.

2.3. The Client shall notify IHQ without delay if it becomes aware of any actual or suspected security breach or unauthorised access that may impact the integrity, availability or confidentiality of IntentOne.

2.4. The Client shall without delay install all updates, upgrades, patches and other corrections which IHQ makes available and not do anything that could reasonably compromise the integrity or security of IntentOne.

2.5. IntentOne utilises third-party services for certain functions, including large language model inferencing, user authentication and feature management. A current list of subprocessors is available at https://intenthq.com/legal/sub-processor-list, as may be updated from time to time.

2.6. In the event IHQ activates incident response mechanisms (including rollback or suspension of Product features), the Client shall cooperate with IHQ's reasonable instructions and shall not attempt to circumvent such measures. IHQ shall notify the Client without undue delay when such mechanisms are activated.

3. LICENCE

3.1. During the Subscription Period and subject to the Client's compliance with the terms of this Agreement (including but not limited to payment of all Fees), IHQ hereby grants Client a limited, non-assignable, non-transferable, non-exclusive licence to use IntentOne in accordance with any usage limits or restrictions set out in the Order Form, solely for Client's internal business operations.

3.2. IHQ reserves all other rights. The Client shall not (and shall not permit any third party to): (i) copy, modify or create derivative works of IntentOne; (ii) reverse engineer, disassemble or decompile IntentOne; (iii) sublicense, sell, lease, distribute or make IntentOne available to any third party; (iv) use IntentOne to develop a competing product or service; or (v) remove or alter any proprietary notices on IntentOne, all except as expressly permitted in the Order Form.

3.3. IntentOne is provided as a hosted SaaS platform and may include access to APIs, SDK components and associated Documentation.

PRODUCT SPECIFIC TERMS – INTENT ONE

4. AUTOMATED AND AI-ASSISTED FEATURES

4.1. Where enabled, IntentOne may operate in different autonomy modes such as Manual, Assisted or Supervised Autonomy (the "**Operating Mode**"), as described in the Documentation. Additional autonomy modes may be made available in future releases. The Client is solely responsible for selecting the applicable Operating Mode and configuring any associated guardrails, thresholds or approval requirements.

5. CLIENT OBLIGATIONS

5.1. The Client acknowledges that the quality, completeness and accuracy of the Client Data it submits or processes through IntentOne directly affects the performance, outputs and functionality of IntentOne. The Client shall:

5.1.1. be solely responsible for ensuring all Client Data provided to IntentOne is accurate, complete, fit for purpose, lawful and that the Client has all necessary rights, consents and permissions in respect of the Client Data;

5.1.2. configure and use IntentOne strictly in accordance with the Documentation and any other instructions communicated by IHQ from time to time;

5.1.3. ensure that any integrations (including SDK or APIs) are implemented correctly and properly maintained;

5.1.4. where the Client has selected an Operating Mode requiring human review, ensure that all Outputs and AI Outputs are reviewed and verified by a human before being used or relied on; and where the Client has selected an Operating Mode permitting autonomous action, ensure that it has configured guardrails, thresholds and approval requirements appropriate to the decisions being taken, and that human intervention is available in respect of any decision which produces legal effects concerning an individual or similarly significantly affects them; and

5.1.5. at all times be responsible for all activities undertaken using its accounts and access credentials.

5.2. Where the Client uses SDK or device-level integrations:

5.2.1. the Client shall ensure implementation complies with applicable laws (including privacy and data protection laws);

5.2.2. the Client shall maintain appropriate user disclosures and consent mechanisms; and

5.2.3. the Client shall ensure all applications or digital properties incorporating the SDK comply with this Agreement.

5.3. The Client is solely responsible for:

5.3.1. decisions it takes based on Outputs and AI Outputs generated by IntentOne;

5.3.2. campaign content, targeting and compliance with applicable laws and regulations; and

5.3.3. any downstream execution of Outputs and AI Outputs in third-party systems.

5.4. The Client acknowledges that:

5.4.1. Outputs and AI Outputs are generated using probabilistic models and require validation;

5.4.2. Outputs and AI Outputs are dependent on the quality, completeness and timeliness of the Client Data; and

5.4.3. IHQ shall have no liability for any deficiency in IntentOne's performance, outputs, or results to the extent arising from or attributable to Client Data that is inaccurate, incomplete, misleading or otherwise deficient, and IHQ does not guarantee specific business outcomes or performance improvements.

5.5. Where Outputs and AI Outputs are exported to third-party systems, the Client is solely responsible for, and IHQ shall have no liability for:

5.5.1. correct implementation and use in those systems;

5.5.2. ensuring compatibility and compliance with third-party requirements.

5.6. The Client shall not use the Product in a manner that:

5.6.1. is excessive or abusive; or

5.6.2. materially exceeds reasonable usage patterns.

PRODUCT SPECIFIC TERMS – INTENT ONE

5.7. IHQ may monitor usage and take reasonable steps (including suspension or throttling) to prevent misuse or degradation of the Product.

6. INDEMNITY

6.1. In addition to Clause 17.4 of the General Terms, the Client shall indemnify, defend and hold harmless IHQ and its Indemnified Parties from and against any Claims arising out of or in connection with:

6.1.1. any unauthorised access, security breach, cyberattack or data loss occurring within the Client Environment, including but not limited to breaches resulting from inadequate security controls, misconfiguration or failure to implement necessary security updates;

6.1.2. any campaigns activated through IntentOne or via third-party systems using audiences, parameters or content exported from IntentOne, including any Claims relating to breach of applicable marketing, consent or communications laws (including unsolicited messaging, timing or frequency violations), in each case based on Client-configured Inputs;

6.1.3. any Claims brought by third parties (including regulatory authorities) arising from (i) security failures within the Client Environment that impact the performance, availability or security of IntentOne, or (ii) Client's failure to obtain specific user consents and/or otherwise comply with applicable privacy or data protection laws; or

6.1.4. any inaccurate, incomplete or outdated suppression lists, opt-out records or frequency controls provided or configured by the Client.

7. CLIENT DATA AND PROCESSING

7.1. Data retention, access and deletion in connection with IntentOne shall be governed by the Data Processing Addendum and the applicable provisions of the General Terms.

8. THIRD-PARTY DEPENDENCIES

8.1. IntentOne utilises third-party services for certain functions, including large language model inferencing, user authentication and feature management. Sub-processors engaged in connection with IntentOne are governed by the Data Processing Addendum.

8.2. IntentOne may integrate with third-party systems (including campaign tools, CRM systems or data sources).

8.3. The Client acknowledges that:

8.3.1. such integrations may be subject to third-party terms;

8.3.2. IHQ is not responsible for the performance, availability or security of third-party systems;

8.3.3. changes in third-party systems may impact the functionality of IntentOne.

8.4. Where IntentOne relies on third-party large language models to generate content, recommendations or analysis, IHQ shall not be liable for Outputs and AI Outputs that violate the third-party provider's usage policies, provided IHQ has implemented reasonable controls to prevent such violations. IHQ shall make available to the Client, through the Documentation or the IHQ Legal Resource Centre, a summary of any third-party usage policies that impose restrictions on permissible use of IntentOne's AI features.

8.5. Where enabled, IntentOne may use feature flags or A/B testing to vary Product functionality for the purpose of improving IntentOne. IHQ shall not Process personal data comprised in the Client Data for the purpose of such experimentation other than on the Client's documented instructions, and the Client may disable experimentation involving personal data at any time by written notice to IHQ. Experimentation which does not involve the Processing of personal data may be conducted at IHQ's discretion. The Client remains solely responsible for campaign outcomes during any experimentation which it has enabled.

8.6. IHQ shall not be liable for variations in IntentOne recommendations, audience composition or campaign performance attributable to feature experimentation, provided such experimentation does not materially degrade the core functionality described in the Documentation.

9. TERMINATION

9.1. Upon termination or expiry of this Agreement and/or IntentOne, the Client shall:

PRODUCT SPECIFIC TERMS – INTENT ONE

9.1.1. cease all use of the IntentOne Product and delete all copies of IntentOne, including backup copies, from its systems and environments;

9.1.2. disable any integrations or SDK components where applicable; and

9.1.3. comply with Clause 15 (Effect of Termination) of the General Terms.

10. SUSPENSION AND REMOVAL OF ACCESS

Without prejudice to Clause 13 (Suspension) of the General Terms, IHQ may suspend or restrict access where:

10.1. the Client's use presents or is in the reasonable opinion of IHQ likely to present a security, legal, or operational risk;

10.2. the Client breaches these Product Specific Terms; or

10.3. continued use may adversely impact IntentOne or other customers.

11. INTENTONE AI ACCEPTABLE USE POLICY

11.1. The Client shall not, and shall ensure that all authorised users shall not:

11.1.1. alter, hide or remove any Intellectual Property Rights notice contained in IntentOne;

11.1.2. reverse engineer, decompile, disassemble or create derivative works from IntentOne, except where permitted by law solely to achieve interoperability, or to make backup copies as necessary for lawful use;

11.1.3. use IntentOne to provide hosting or SaaS offerings to third parties, or to create a competing product or service;

11.1.4. transfer, assign or sublicense IntentOne without prior written consent from IHQ;

11.1.5. use IntentOne in violation of applicable laws or in any harmful, threatening, defamatory, obscene or discriminatory manner;

11.1.6. circumvent any access control, security or privacy features of IntentOne;

11.1.7. extract algorithms, workflows or hierarchies from IntentOne to create competitive substitutes;

11.1.8. use IntentOne to create software containing Malicious Software or to damage or intercept any system or data;

11.1.9. train any algorithms using outputs, data or behavioural patterns extracted from IntentOne;

11.1.10. configure compliance controls to circumvent applicable laws, or fail to maintain accurate suppression lists and opt-out records;

11.1.11. use audience segmentation or targeting features in a manner that discriminates on the basis of protected characteristics under applicable law;

11.1.12. disable or override compliance suppressions enforced at runtime;

11.1.13. where IntentOne is provided on an "unlimited" basis, use it excessively or in a manner materially exceeding reasonable expectations; IHQ may take proportionate steps, including suspension, with reasonable prior written notice except where immediate action is required; and

11.1.14. rely on IntentOne as the sole basis for high-risk or legally binding decisions without appropriate human oversight.

11.2. The Client shall ensure all Client Data provided to IHQ is free from any Malicious Software.