1NCE AI Acceptable Use Policy (version as of July 2026)

This Acceptable Use Policy ("AI AUP") forms part of the contractual documentation for the 1NCE AI service and supplements 1NCE's general Acceptable Use Policy ("General AUP", Version 2025_12 or any subsequent version). This AI AUP applies in addition to the General AUP to the extent the Customer uses 1NCE AI. Where this AI AUP deviates from or supplements the General AUP, this AI AUP prevails with respect to the 1NCE AI service only and only to the extent of the deviation. This AI AUP is incorporated by reference into the Service-Specific Terms for 1NCE AI (Part B) and is binding upon the Customer and its Users. The order of precedence set out in Section 1.4 of Part A applies.

1. Scope and Application

1.1 This AI AUP governs the use by the Customer and its Users of the 1NCE AI service (hereinafter referred to as the "Service" or "1NCE AI"), including any associated APIs, customer portals, embedding models, and related features (collectively, together with the underlying AI Models, the "AI Services"). Terms and expressions not defined in this AI AUP shall have the meanings assigned to them in the Service-Specific Terms for 1NCE AI ("Part B"), in Part A of the GTC, or in the General AUP.

1.2 This AI AUP applies to the Customer, to any persons authorized by the Customer to access the Service (including employees, contractors, agents, and end users of applications built by the Customer using the Service), and to any Inputs submitted to, and Outputs generated by, the Service (collectively, the "Users"). The Customer shall ensure that all Users comply with this AI AUP at all times.

1.3 The Customer acknowledges that the AI Services are subject to multiple layers of policy obligations, including (a) this AI AUP; (b) the General AUP; (c) the terms and acceptable use, usage, or responsible-AI policies of the underlying infrastructure provider (in particular Amazon Web Services); and (d) the terms and acceptable use, usage, or responsible-AI policies of the relevant Model Providers (in particular, as applicable, Anthropic, Meta, Mistral, and Amazon). The Customer undertakes to comply with all such policies as applicable to the AI Models it accesses through the Service. A violation of any such upstream policy is deemed a violation of this AI AUP.

1.4 The purpose of this AI AUP is to: (a) ensure that the AI Services are used in compliance with applicable law, including in particular Regulation (EU) 2024/1689 ("EU AI Act") and Regulation (EU) 2016/679 ("GDPR"); (b) protect the integrity, security, and availability of 1NCE's infrastructure and that of its upstream providers; (c) ensure compliance with the terms imposed on 1NCE by upstream infrastructure and Model Providers; and (d) promote the responsible and lawful use of artificial intelligence by the Customer and its Users.

1.5 The lists of prohibited uses and content set out in this AI AUP are illustrative and not exhaustive. 1NCE may update this AI AUP from time to time in accordance with Section 12 of Part A.

2. General Prohibitions

2.1 The Customer shall not use, and shall not permit any User to use, the AI Services in any manner that is unlawful, fraudulent, infringing, deceptive, harmful, or otherwise contrary to this AI AUP, the General AUP, applicable law, the EU AI Act, the GDPR, or the applicable terms of any upstream infrastructure or Model Provider.

2.2 Without limitation to Section 2.1, the Customer shall not use, and shall not permit any User to use, the AI Services to:

a) engage in, promote, facilitate, plan, incite, or further any illegal or unlawful activity, including violence, terrorism, human trafficking, the illegal distribution of controlled substances, or any criminal conduct;

b) infringe, misappropriate, or otherwise violate any third-party rights, including intellectual property rights, rights of privacy,

publicity, or personality, or any contractual or fiduciary obligations;

c) generate, solicit, or disseminate child sexual abuse material ("CSAM"), any sexual content involving minors, or any content that sexualises, grooms, exploits, or endangers minors; the Customer acknowledges 1NCE's zero-tolerance policy and 1NCE's right and, where applicable, duty to report such material to the competent authorities;

d) develop, design, manufacture, market, or operate weapons, including chemical, biological, radiological, nuclear, or high-yield explosive ("CBRN") weapons, conventional weapons used in a manner that could cause death or serious bodily harm, or to perform a lethal function in a weapon without meaningful human authorization or control;

e) engage in, facilitate, or plan activities that could compromise, damage, disrupt, or attack critical infrastructure (including energy, water, transportation, financial, healthcare, or telecommunications infrastructure);

f) create, distribute, or facilitate malware, viruses, ransomware, spyware, or other malicious code; engage in network intrusion or unauthorised access; circumvent, disable, or interfere with security mechanisms, content filters, safety features, or rate limits of the Service or of any underlying AI Model; or use the Service to identify vulnerabilities, perform unauthorised security testing, reverse-engineer, or evade safeguards;

g) engage in fraud, scams, phishing, spam, deceptive marketing, or unsolicited bulk communications, or to generate or disseminate disinformation, including content designed to mislead the public, manipulate elections, or undermine democratic processes;

h) harass, bully, threaten, intimidate, defame, or incite hatred or violence against any individual or group, including on the basis of race, ethnicity, national origin, religion, sex, sexual orientation, gender identity, age, disability, or any other characteristic protected by applicable law;

i) promote, encourage, or facilitate self-harm, suicide, eating disorders, or other harmful behaviours; provide instructions for, or otherwise enable, such acts;

j) compromise the privacy or identity rights of any person, including through unlawful surveillance, tracking, profiling, scraping of personal data, facial recognition, biometric identification or categorisation, emotion recognition, or the inference of sensitive personal attributes, in each case other than as permitted by applicable law;

k) impersonate any person or entity, falsely represent affiliation with any person or entity, or otherwise engage in deceptive practices regarding the source or authorship of Inputs or Outputs;

l) generate or disseminate non-consensual sexual imagery, including realistic depictions of identifiable persons, or non-consensual intimate imagery of any kind;

m) generate Outputs that purport to provide professional advice in medical, legal, financial, regulatory, or other expert domains in a manner that holds out the Output as professional advice without appropriate human professional review and the disclosures required by applicable law;

n) submit as Inputs, or extract through Outputs, trade secrets, confidential information, or proprietary information of any third party that the Customer is not authorized to process; or

o) engage in any other activity that violates the General AUP, the terms of an applicable Model Provider, or the AWS Acceptable Use Policy or AWS Responsible AI Policy.

3. EU AI Act – Prohibited and High-Risk Practices

3.1 The Customer shall not use, and shall not permit any User to use, the AI Services for any practice prohibited under Article 5 of the EU AI Act. Without limitation, the Customer shall not use the AI Services to:

a) deploy subliminal techniques beyond a person's consciousness, or purposefully manipulative or deceptive techniques, with the objective or effect of materially distorting the behaviour of a person or group in a manner that causes, or is reasonably likely to cause, significant harm;

b) exploit any of the vulnerabilities of a person or group of persons due to their age, disability, or specific social or economic situation in a manner that materially distorts behaviour and causes, or is reasonably likely to cause, significant harm;

c) evaluate or classify natural persons or groups of persons over a period of time based on their social behaviour or personality characteristics, where this leads to detrimental or unfavourable treatment of those persons ("social scoring");

d) make risk assessments of natural persons in order to assess or predict the risk of a natural person committing a criminal offence, based solely on profiling or personality traits;

e) create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;

f) infer emotions of a natural person in the areas of workplace and education institutions, except where the use is intended to be put in place or into the market for medical or safety reasons;

g) biometrically categorise natural persons to deduce or infer race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation;

h) undertake "real-time" remote biometric identification of natural persons in publicly accessible spaces for the purposes of law enforcement, save where authorised under and conducted in strict compliance with Article 5(1)(h) of the EU AI Act.

3.2 The AI Services are not designed, evaluated, validated, or certified for use as, or as part of, a high-risk AI system within the meaning of Article 6 of the EU AI Act, read in conjunction with Annex III thereof. The Customer shall not use the AI Services, and shall not permit any User to use the AI Services, for the development, deployment, or operation of any AI system intended for use in the high-risk areas listed in Annex III of the EU AI Act, including, without limitation: (a) biometrics; (b) critical infrastructure; (c) education and vocational training; (d) employment, workers management, and access to self-employment; (e) access to and enjoyment of essential private and public services and benefits, including credit-worthiness, life and health insurance pricing, and emergency services dispatch; (f) law enforcement; (g) migration, asylum, and border control; and (h) the administration of justice and democratic processes.

3.3 Where the Customer's use of the Service brings the Customer within scope of the obligations of a "provider" or "deployer" of an AI system within the meaning of the EU AI Act, the Customer is solely responsible for complying with those obligations, including (where applicable) the transparency obligations set out in Article 50 of the EU AI Act. In particular, the Customer shall:

a) inform natural persons interacting with an AI system built or operated by the Customer using the Service that they are interacting with an AI system, except where this is obvious from the circumstances and context;

b) where the Customer generates or manipulates image, audio, or video content

constituting a "deep fake" within the meaning of Article 50(4) of the EU AI Act, disclose that the content has been artificially generated or manipulated;

c) where the Customer generates or manipulates text published with the purpose of informing the public on matters of public interest, disclose that the text has been artificially generated or manipulated, save where the content has undergone a process of human review or editorial control and a natural or legal person holds editorial responsibility for the publication; and

d) preserve any provenance, watermark, or content-authentication metadata embedded in or accompanying Outputs and refrain from removing or altering such metadata.

4. Data Protection and Sensitive Inputs

4.1 The Customer shall comply with all applicable data protection and privacy when submitting Inputs to, or processing Outputs from, the Service. The processing of personal data by 1NCE on behalf of the Customer is governed by the 1NCE AI Data Processing Addendum.

4.2 The Customer is responsible for assessing whether Inputs contain personal data, confidential information, or commercially sensitive information, and for implementing appropriate measures (including, where appropriate, pseudonymisation, redaction, or anonymisation) prior to submission. 1NCE bears no responsibility for the inclusion of personal data, special-category data, or other sensitive information in Inputs that have not been expressly agreed to be processed under the AI Services.

5. Flow-Down of Upstream Terms

5.1 The AI Services rely on third-party infrastructure and Model Providers. The Customer acknowledges and agrees that:

a) the AWS Acceptable Use Policy and the AWS Responsible AI Policy, as amended from time to time, apply to the underlying infrastructure that supports the Service, and the Customer shall not use the Service in any manner that would, if used directly with AWS, constitute a breach of those policies;

b) each Model Provider may impose its own usage, acceptable-use, or responsible-AI policy in respect of the AI Models it makes available, including those of Anthropic, Meta, Mistral, and Amazon, and the Customer shall comply with such policies in respect of each AI Model it accesses through the Service; in particular, the Customer acknowledges that (i) Anthropic's Usage Policy is enforced against users accessed through authorised resellers and passthrough access; (ii) Meta's Llama acceptable-use policies may impose territorial, multimodal, or end-user restrictions, including specific restrictions affecting EU-domiciled entities and certain multimodal Llama variants; and (iii) Mistral's Usage Policy scope varies by deployment model, and the applicable terms for Mistral models accessed through the Service are those that bind 1NCE under the relevant Bedrock or other distribution channel;

c) the current list of applicable upstream policies, together with the AI Models offered through the Service, is published in or accessible through the Service Description or the Model Catalogue and is updated from time to time;

d) a breach by the Customer or any User of any upstream policy referred to in this Section 5 shall constitute a breach of this AI AUP, and 1NCE is entitled to take the enforcement actions set out in Section 8 below; and

e) where an upstream provider requires 1NCE to suspend, restrict, or terminate access to a specific AI Model, or to a specific Customer or User, 1NCE is entitled to comply with such requirement without liability to the Customer.

5.2 Nothing in this Section 5 grants the Customer any rights against, or recourse to, the upstream infrastructure or Model Providers beyond those expressly conferred by the relevant Model Provider terms.

6. Security and Integrity of the Service

6.1 The Customer shall not, and shall not permit any User to:

a) damage, interfere with, overburden, or otherwise adversely impact the availability, reliability, integrity, or security of the AI Services, of 1NCE's systems, or of the systems of any third party;

b) attempt to circumvent or breach any security, authentication, or rate-limiting mechanism of the AI Services, including the use of multiple accounts or API keys to evade Rate Limits or spend controls;

c) submit Inputs designed to elicit responses that would, if generated, violate this AI AUP, an upstream policy, or applicable law, including through prompt-injection, jailbreaking, or similar techniques;

d) use the AI Services to perform unauthorised testing, benchmarking, reverse-engineering, decompilation, or extraction of model weights or training data; or

e) use the AI Services in conjunction with any third-party service, application, or system in a manner that would breach the obligations of the Customer under this AI AUP or the underlying Contract.

6.2 The Customer shall implement appropriate access controls to prevent unauthorised use of its API keys and shall notify 1NCE without undue delay of any actual or suspected compromise of any API key or other credential issued to it for the use of the Service.

7. Specific Requirements for Consumer-Facing and Other Elevated-Risk Uses

7.1 Where the Customer uses the AI Services to build or operate a consumer-facing application, a chatbot, an agent capable of taking autonomous actions, an application directed at or likely to be used by minors, or any other application that may carry an elevated risk of harm to individuals (each, an "Elevated-Risk Application"), the Customer shall, in addition to its other obligations under this AI AUP:

a) implement appropriate human oversight, testing, and content-moderation safeguards proportionate to the risks of the use case;

b) comply with all applicable transparency, disclosure, and age-gating requirements, including those arising under Article 50 of the EU AI Act, the Digital Services Act, and any applicable child-protection legislation;

c) ensure that the Elevated-Risk Application does not represent Outputs as having been generated by a human, and does not deceive end users as to the artificial nature of the system;

d) comply with the elevated-risk requirements (where any) of the applicable Model Provider, including, in respect of Anthropic-provided Models, Anthropic's High-Risk Use Case Requirements and Additional Use Case Guidelines as amended from time to time; and

e) upon request from 1NCE, provide information sufficient to demonstrate compliance with this Section 7.

8. Monitoring, Suspension, and Enforcement

8.1 1NCE reserves the right, but is not obliged, to monitor the use of the AI Services for the purpose of detecting violations of this AI AUP, applicable law, or applicable upstream policies. Where 1NCE acts as a data processor in respect of personal data contained in Inputs or Outputs, any such monitoring shall be conducted in accordance with the 1NCE AI Data Processing Addendum and on a case-by-case basis (anlassbezogen im Einzelfall)

only where there is a concrete and documented suspicion of a violation.

8.2 Where 1NCE identifies, or reasonably suspects, a violation of this AI AUP, 1NCE may, at its sole discretion and in accordance with Section 3.7 of Part A and Section 11.3 of Part B, take any or all of the following actions:

a) issue a warning to the Customer requiring it to remedy the violation;

b) restrict the Customer's access to specific features, AI Models, or use cases;

c) temporarily suspend the Customer's access to the Service in whole or in part;

d) block or modify Inputs or Outputs that violate this AI AUP;

e) in the event of a material breach, terminate the Contract for good cause (außerordentliche Kündigung aus wichtigem Grund); and/or

f) report the violation to the competent regulatory or law-enforcement authorities, where required by applicable law (including in respect of CSAM).

8.3 Where feasible and consistent with applicable law and the protection of 1NCE's legitimate interests, 1NCE shall give the Customer notice of an AUP violation and a reasonable opportunity to remedy the violation before taking enforcement action. However, 1NCE is entitled to act immediately and without prior notice where necessary to protect its infrastructure or that of an upstream provider, to comply with applicable law or an upstream policy, to prevent harm to third parties, or to comply with an order or instruction from a competent court, regulatory authority, or upstream provider.

8.4 The Customer shall promptly notify 1NCE of any actual or suspected violation of this AI AUP of which it becomes aware, and shall cooperate with 1NCE in all reasonable efforts to prevent, stop, investigate, or remedy such violations, including by providing information reasonably necessary for 1NCE to comply with its own obligations to upstream providers or competent authorities.

9. Reporting of Violations

9.1 Suspected violations of this AI AUP, including the misuse of the AI Services by third parties, may be reported to 1NCE at [●]. Reports concerning CSAM or imminent harm to natural persons should be marked as such and will be handled with priority.

10. Liability and Indemnity

10.1 Without prejudice to Section 10 of Part B, the Customer shall indemnify and hold harmless 1NCE and its affiliates, directors, officers, and employees on first demand (auf erstes Anfordern) from and against all third-party claims, losses, damages, liabilities, fines, penalties, and associated costs (including reasonable legal defence costs) arising from or in connection with any breach of this AI AUP by the Customer or any User, or any claim by an upstream infrastructure or Model Provider arising from such breach.

11. Amendments

11.1 1NCE may amend this AI AUP in accordance with Section 12 of Part A, in particular where required to reflect (a) changes to applicable law (including changes in the interpretation or enforcement of the EU AI Act and the GDPR); (b) changes to the upstream infrastructure or Model Provider policies referred to in Section 5; or (c) the addition, modification, or discontinuation of AI Models in the Model Catalogue.