



END USER LICENSE AGREEMENT FOR MAGONEAI

(AWS Marketplace)

Effective Date: 22nd June 2026

Licensor: Magure Tech Middle East Ltd, a company incorporated under the laws of the Dubai International Financial Centre (DIFC), registration number CL8230, registered office at Unit 195, Level 1, Gate Avenue – South Zone, DIFC, Dubai, UAE (“Magure”, “we”, “us”).

PREAMBLE – PLEASE READ CAREFULLY

This End User License Agreement (this “Agreement” or “EULA”) is a binding legal agreement between Magure and the legal entity or person that subscribes to, accesses, installs, deploys, or uses the Software (defined below) through AWS Marketplace (“Customer”, “you”). Magure and Customer are each a “Party” and together the “Parties”.

By subscribing to the Software through AWS Marketplace, clicking “Accept” (or a similar control), or by installing, deploying, accessing, or using the Software, you agree to be bound by this Agreement. If you are entering into this Agreement on behalf of a company or other legal entity, you represent that you have authority to bind that entity, and “Customer” refers to that entity. **If you do not have such authority, or do not agree to these terms, do not subscribe to, install, or use the Software.**

Relationship to AWS. The Software is offered by Magure, not by Amazon Web Services, Inc. or its affiliates (“AWS”). AWS is not a party to this Agreement and is not the licensor of the Software. Your procurement, billing, metering, and transaction relationship for the Software is governed by your agreement with AWS, including the AWS Customer Agreement and the AWS Service Terms (collectively, the “AWS Agreement”). This Agreement governs the license to, and your use of, the Software as between Magure and Customer. In the event of a conflict between this Agreement and the AWS Agreement with respect to the rights and obligations between Magure and Customer regarding the Software, this Agreement controls solely as between Magure and Customer; nothing in this Agreement modifies the AWS Agreement or AWS’s relationship with Customer.

1. DEFINITIONS

In this Agreement, capitalised terms have the meanings set out below:

“Affiliate” means any entity that controls, is controlled by, or is under common control with a Party.

“Authorised User” means Customer’s employees, contractors, and Affiliates’ personnel authorised by Customer to use the Software.

“AWS Marketplace” means the online software marketplace operated by AWS through which Customer subscribes to the Software.

“Confidential Information” means non-public information disclosed by a Party that is marked confidential or would reasonably be understood to be confidential, including the Software, Documentation, and non-public technical and commercial information.

“Customer Application” means applications, workflows, automations, integrations, prompts, configurations, agents, knowledge bases, and business logic created by or on behalf of Customer using the Software or its APIs.

“Customer Cloud Environment” means in a Self-Hosted Deployment, the AWS account(s) and associated cloud, hybrid, or on-premise infrastructure designated and controlled by Customer within which the Software is deployed.

“Customer Data” means data, content, information, and inputs provided by or on behalf of Customer to the Software, including data ingested into knowledge bases and inputs to agents.

“Documentation” means Magure’s then-current product documentation for the Software.

“End User” means an end customer or end user of Customer’s services who interacts with a Customer Application.

“Foundation Model” means any foundation model, large language model, or similar AI model invoked through the Software’s model gateway, whether (a) hosted by a third-party provider (e.g., OpenAI, Anthropic, Amazon Bedrock, Google, Meta, Mistral); (b) an open-source or open-weight model deployed by Customer; or (c) a model fine-tuned, customised, or developed by or for Customer.

“Hosted Deployment” means a delivery model in which Magure (or its hosting subprocessor) hosts and operates the Software and Customer accesses it as a service.

“Intellectual Property Rights” means all intellectual property rights worldwide, registered or unregistered, including patents, trademarks, copyright, design rights, database rights, trade secrets, and know-how, and applications for them.

“Magure Technology” means the Software, its underlying software, APIs, SDKs, agent frameworks, orchestration engines, models proprietary to Magure, templates, system logic, user interfaces, Documentation, and all underlying, embedded, or derivative technology, including updates and enhancements, but excluding Customer Applications and Customer Data.

“Order” means a subscription, contract, or transaction for the Software placed by Customer through AWS Marketplace, including any private offer accepted by Customer.

“Output” means content, predictions, recommendations, analyses, or results generated by the Software (including by AI agents or Foundation Models) in response to inputs.

“Personal Data” means information relating to an identified or identifiable natural person, as defined under applicable law.

“Self-Hosted Deployment” means a delivery model in which the Software is provided as a machine image (AMI), container, or similar package that Customer deploys and operates within the Customer Cloud Environment.

“Software” means MagOneAI, Magure’s enterprise agentic AI platform, in the form made available through AWS Marketplace (whether as a Self-Hosted Deployment or a Hosted Deployment), including its components, modules, features, agents, tools, APIs, and updates, together with the Documentation.

“Subscription Term” means the period of Customer’s subscription to the Software as set out in the applicable Order through AWS Marketplace.

2. LICENSE GRANT AND DELIVERY MODELS

2.1 License Grant. Subject to Customer's compliance with this Agreement and payment of all applicable fees through AWS Marketplace, Magure grants Customer a non-exclusive, non-transferable, non-sublicensable, right, during the Subscription Term, for its Authorised Users to access and use the Software for Customer's internal business purposes, in accordance with the Documentation and the scope, capacity, and entitlements specified in the applicable Order.

2.2 Delivery Models. The Software may be made available through AWS Marketplace as a Self-Hosted Deployment, a Hosted Deployment, or both. The applicable model is identified on the product listing or Order. Sections 3 and 4 allocate responsibilities accordingly.

2.3 Reservation of Rights. Magure reserves all rights not expressly granted. No rights are granted by implication, estoppel, or otherwise. This Agreement does not constitute a sale of the Software or of any copy of it, and Customer acquires no ownership interest in the Magure Technology.

3. SELF-HOSTED DEPLOYMENT – RESPONSIBILITIES

Where the Software is provided as a Self-Hosted Deployment:

3.1 The Software is deployed and operated within the Customer Cloud Environment. Customer is responsible for: (a) procuring and paying for all underlying infrastructure (compute, storage, networking, GPU, database, observability) and all Foundation Model API consumption, billed by AWS and/or the relevant providers and not included in the fees for the Software; (b) maintaining the security, availability, patching, and configuration of the Customer Cloud Environment up to the application layer; (c) granting Magure least-privilege, time-bound access (if any) required to provide support; and (d) backups, disaster recovery, and business continuity, unless expressly purchased from Magure.

3.2 Magure is responsible for providing the Software, updates, security patches, and bug fixes within the application layer in accordance with this Agreement and any applicable support terms.

3.3 Customer Data Location. In a Self-Hosted Deployment, Customer Data resides at all times within the Customer Cloud Environment under Customer's control and does not leave that environment except as directed or configured by Customer (for example, where Customer integrates the Software with external systems or Foundation Model providers of Customer's choosing). Magure does not host, transmit, or store Customer Data on Magure-controlled infrastructure as part of a standard Self-Hosted Deployment.

4. HOSTED DEPLOYMENT – RESPONSIBILITIES

Where the Software is provided as a Hosted Deployment:

4.1 Magure (or its hosting subprocessor) is responsible for hosting, operating, securing, and maintaining the Software environment at the application and infrastructure layers within its control, in accordance with Magure's information security programme described in Section 9 and any applicable service levels.

4.2 Customer remains responsible for: (a) its Authorised Users and credentials; (b) Customer Data and its legality and accuracy; (c) Customer Applications and configurations; and (d) any Foundation Model providers or third-party services Customer elects to connect.

4.3 Foundation Model API consumption and any Customer-elected third-party services are billed by the relevant providers and are not included in the fees for the Software unless expressly stated in the Order.

5. ORDERS, FEES, BILLING, AND TAXES (VIA AWS MARKETPLACE)

5.1 Billing Through AWS. All fees for the Software are set out in the applicable AWS Marketplace listing or Order and are billed, collected, and remitted through AWS Marketplace in accordance with the AWS

Agreement. Magure does not invoice Customer directly for AWS Marketplace transactions except where expressly agreed in a private offer.

5.2 Foundation Model and Infrastructure Costs. Customer pays all Foundation Model API consumption and underlying cloud infrastructure costs directly to AWS and/or the relevant providers. These costs are separate from, and not included in, the fees for the Software.

5.3 Taxes. Fees are exclusive of taxes, duties, and withholdings except taxes on Magure's net income. Responsibility for transaction taxes is determined by the AWS Agreement and applicable law.

5.4 Refunds. Except as required by applicable law or expressly provided in this Agreement, fees are non-refundable. Any refund is handled in accordance with the AWS Marketplace refund process and Magure's refund policy as published on the listing.

5.5 Renewals and Price Changes. Subscriptions renew, and prices may change, as stated on the AWS Marketplace listing or Order. Renewal pricing for negotiated private offers may be subject to an annual increase of up to five percent (5%).

6. CUSTOMER RESPONSIBILITIES AND ACCEPTABLE USE

6.1 Customer is responsible for the acts and omissions of its Authorised Users and for safeguarding all access credentials.

6.2 Acceptable Use. Customer shall not, and shall not permit any user to: (a) use the Software for any unlawful, harmful, fraudulent, or infringing purpose; (b) reverse-engineer, decompile, disassemble, or attempt to derive the source code, model weights, or underlying structure of the Software, except to the extent this restriction is prohibited by applicable law; (c) copy, modify, create derivative works of, distribute, sell, resell, rent, lease, sublicense, or otherwise make the Software available to any third party, except as expressly permitted; (d) circumvent or disable any license key, security, authentication, rate-limiting, metering, or model-safety controls, or use the Software beyond the entitlements in the Order; (e) use the Software to develop or train a competing product or service, or to benchmark for competitive purposes; (f) introduce viruses, malware, or harmful code into the Software; (g) remove, obscure, or alter any proprietary notices; (h) use the Software for prohibited AI practices under applicable law (e.g., social scoring, real-time biometric mass surveillance, or manipulative or exploitative AI); or (i) use the Software to make fully autonomous decisions producing legal or similarly significant effects on individuals (including credit, employment, healthcare, insurance, justice, or law enforcement) without meaningful human oversight.

6.3 Customer Data. Customer is responsible for the accuracy, legality, and quality of Customer Data; for obtaining all necessary rights, consents, and notices; and for classifying data sensitivity (e.g., PII, PHI, financial) and configuring the Software's access controls accordingly.

6.4 License Compliance and Verification. Customer shall not exceed the licensed scope or capacity. Magure may employ technical measures to verify compliance and, on reasonable notice, may verify Customer's use; under-licensing discovered shall be trued-up through AWS Marketplace.

7. FOUNDATION MODELS

7.1 Model-Agnostic Design. The Software is model-agnostic and supports Foundation Models that are (a) third-party hosted and accessed via API, (b) open-source or open-weight and deployed by Customer, or (c) fine-tuned or proprietary to Customer. Magure provides the integration, gateway, orchestration, observability, and evaluation capabilities of the Software, but is not the developer or licensor of any underlying Foundation Model unless Magure expressly identifies a model as a Magure-developed model in the Order.

7.2 Third-Party Model Providers. Customer selects and enables Foundation Model providers, subscribes to them directly, and holds the contractual relationship with each. Customer is responsible for: (a) accepting each provider's terms and acceptable-use policies; (b) ensuring the chosen models are appropriate for Customer's data sensitivity and regulatory requirements; (c) monitoring provider availability, model deprecations, and policy changes; and (d) any data processing performed by such providers on data Customer sends through the Software. Magure is not responsible for the acts, omissions, availability, accuracy, security, data handling, or changes of any Foundation Model provider.

7.3 Customer-Deployed Models. Where Foundation Models are deployed by Customer (open-source, open-weight, fine-tuned, or proprietary), Customer is responsible for the model's deployment, configuration, performance, availability, security, licence compliance, and lifecycle. Magure's responsibility is limited to integration of the model with the Software and does not extend to the model itself, its weights, its outputs, or its behaviour. Open-source and open-weight models are subject to their own licence terms, with which Customer is solely responsible for complying.

8. INTELLECTUAL PROPERTY

8.1 Magure Technology. Magure and its licensors retain all right, title, and interest, including all Intellectual Property Rights, in and to the Magure Technology. No ownership transfers to Customer by virtue of this Agreement or Customer's use of the Software.

8.2 Customer Data and Customer Applications. As between the Parties, Customer retains all right, title, and interest, including all Intellectual Property Rights, in and to Customer Data and to assets created by or on behalf of Customer using the Software, including workflows, agents and agent configurations, prompts and prompt templates, knowledge bases and retrieval indices, integrations and tool configurations, custom interfaces, and other Customer Applications (collectively, "Customer Build-on Assets"). Magure claims no ownership of Customer Build-on Assets, and Customer's ownership survives termination.

8.3 Outputs. As between the Parties, Customer owns the Outputs generated by the Software from Customer's inputs, subject to (a) Foundation Model provider terms and (b) the inherent nature of generative AI (multiple users may receive similar Outputs from similar inputs, and Outputs may not be unique or copyrightable in all jurisdictions).

8.4 No Training on Customer Data. Magure shall not use Customer Data, Customer Applications, or Outputs to train, fine-tune, or improve the Software, any Foundation Model, or any model offered to other customers, except (a) with Customer's prior written consent or (b) for Customer's exclusive benefit. Magure may use aggregated and anonymised operational metrics for security, performance, capacity planning, and service improvement, provided no Customer Data, Customer Applications, or Personal Data are identifiable.

8.5 Fine-Tuned Model Weights. Where Customer fine-tunes or customises a Foundation Model using Customer Data, the resulting fine-tuned weights are Customer's property, subject only to the licence terms of any underlying open-source or open-weight base model. Magure claims no ownership of Customer's fine-tuned weights.

8.6 Feedback. Magure may freely use feedback Customer provides to improve the Software, provided such use does not disclose Customer's Confidential Information, Customer Data, or Customer Applications.

9. DATA PROTECTION AND SECURITY

9.1 Compliance. Each Party shall comply with the data protection and privacy laws applicable to it in connection with this Agreement. Customer is solely responsible for determining which data protection and

privacy laws apply to Customer Data and to Customer's use of the Software – in any jurisdiction in which Customer, its Authorised Users, or its End Users operate, or to which Customer Data relates – and for ensuring that its provision of Customer Data to, and use of, the Software complies with those laws, including obtaining all necessary consents and notices and establishing a lawful basis for processing. Where Magure processes Personal Data on Customer's behalf, Magure shall comply with the data protection laws applicable to it as a processor and with the Data Processing Addendum.

9.2 Roles. Customer is the Controller of Personal Data within Customer Data and determines the purposes and means of processing. In a Self-Hosted Deployment, Personal Data remains within the Customer Cloud Environment and Magure does not process it except to the limited extent Customer instructs Magure to provide scoped support, in which case Magure acts as Processor for those limited activities. In a Hosted Deployment, Magure acts as Processor for Personal Data processed on Customer's instructions. Where Magure acts as Processor, the Data Processing Addendum set out in Annex A to this Agreement applies, is incorporated into and forms part of this Agreement, and is binding on Customer.

9.3 Security Programme. Magure operates an information security management system certified to ISO 27001 and an AI governance management system aligned with ISO 42001, and applies controls consistent with such standards (including secure SDLC, least-privilege access, audit logging, and personnel security). In a Self-Hosted Deployment, security of the Customer Cloud Environment (infrastructure, network, account-level IAM, and configuration of the Software within it) is Customer's responsibility, and Magure is not liable for incidents caused by misconfiguration of Customer-controlled infrastructure.

9.4 Security Incidents. Magure shall notify Customer without undue delay (and within seventy-two (72) hours) after becoming aware of a confirmed security incident affecting Customer Data within Magure's control.

9.5 Subprocessors. Where Magure engages subprocessors to process Personal Data on Customer's behalf, Magure shall impose data protection obligations no less protective than those in this Agreement and shall provide reasonable notice of material changes.

10. CONFIDENTIALITY

10.1 Each Party shall use the other's Confidential Information only to perform under this Agreement and shall protect it with no less than reasonable care.

10.2 Exclusions. Confidential Information does not include information that (a) is or becomes public through no fault of the recipient; (b) was known to the recipient before disclosure free of obligation; (c) is independently developed; or (d) is lawfully obtained from a third party without restriction.

10.3 Compelled Disclosure. The recipient may disclose Confidential Information as required by law or court order, with prompt prior notice where legally permitted.

10.4 Survival. Confidentiality obligations survive for five (5) years after termination; trade secrets are protected for as long as they remain trade secrets.

11. WARRANTIES AND DISCLAIMER

11.1 Mutual. Each Party warrants it has authority to enter into this Agreement.

11.2 Limited Software Warranty. Magure warrants that, during the Subscription Term, the Software will materially conform to the Documentation, and that Magure will not knowingly introduce malicious code into the Software. Customer's exclusive remedy for breach of this warranty is, at Magure's option, (a) correction of the non-conformity within a reasonable period or (b) if correction is not commercially feasible, termination

of the affected subscription and a refund (processed through AWS Marketplace) of fees pre-paid for the affected period after the non-conformity was reported.

11.3 DISCLAIMER. EXCEPT AS EXPRESSLY SET OUT IN THIS AGREEMENT, THE SOFTWARE, ANY UPDATES, AND ALL OUTPUTS ARE PROVIDED “AS IS” AND “AS AVAILABLE”. TO THE MAXIMUM EXTENT PERMITTED BY LAW, MAGURE DISCLAIMS ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, AND ANY WARRANTY THAT THE SOFTWARE OR OUTPUTS WILL BE UNINTERRUPTED, ERROR-FREE, SECURE, OR ACCURATE. SECTION 12 GOVERNS AI-SPECIFIC DISCLAIMERS.

12. AI-SPECIFIC PROVISIONS

12.1 Probabilistic Nature. Customer acknowledges that AI is probabilistic, not deterministic. Outputs (a) may contain errors, inaccuracies, biases, or fabricated information (“hallucinations”); (b) are not guaranteed to be accurate, complete, current, or fit for any particular purpose; (c) may vary across executions even with identical inputs; and (d) may change over time as Foundation Models, prompts, knowledge bases, or Software components are updated.

12.2 Human Oversight. Customer is responsible for establishing appropriate human oversight, review, and approval before relying on, publishing, or making consequential decisions based on Outputs. Customer shall not deploy Outputs in high-risk use cases (legal, medical, financial, safety-critical, employment, credit, or justice) without qualified human review.

12.3 No Professional Advice. Outputs do not constitute legal, medical, financial, tax, or other professional advice, and Customer shall not represent Outputs as advice from Magure.

12.4 Customer’s AI Compliance. Customer is solely responsible for determining whether, and for ensuring that, its use of the Software and the Outputs complies with all laws, regulations, and regulatory guidance applicable to Customer in any jurisdiction in which Customer, its Authorised Users, or its End Users operate – including any laws governing artificial intelligence, automated decision-making, data protection, consumer protection, and sector-specific activities. Customer is solely responsible for fulfilling any obligations imposed on it as a deployer or user of AI systems under such laws, including any transparency notices, risk or impact assessments, record-keeping, and post-deployment monitoring.

12.5 Bias and Fairness. While the Software supports controls, evaluations, and guardrails, Magure does not warrant that Outputs will be free of bias. Customer is responsible for evaluating Outputs for bias relative to its specific use case and population.

12.6 Auditability. The Software provides audit logs and traceability features consistent with its “Auditable by Design” principle to support Customer’s oversight and regulatory obligations.

13. SUPPORT

Support is provided as described on the AWS Marketplace listing, the Documentation, or an applicable support schedule or private offer. Unless otherwise stated, service levels and service credits apply only to defects attributable to the Software and exclude issues caused by the Customer Cloud Environment, Customer Applications or configurations, Foundation Model providers, Customer-Deployed Models, scheduled maintenance, or force majeure.

14. INDEMNIFICATION

14.1 By Magure. Magure shall defend Customer against third-party claims alleging that the Magure Technology, as provided by Magure and used in accordance with this Agreement, infringes that third party's Intellectual Property Rights, and shall pay damages and reasonable costs finally awarded or agreed in settlement. Magure's obligations do not apply to claims arising from (a) Customer Data; (b) Outputs; (c) Customer Applications; (d) use of the Software in combination with non-Magure products or services where the claim would not have arisen but for the combination; (e) Customer's modifications; (f) use after notice to discontinue or after provision of a non-infringing alternative; (g) Foundation Model provider IP claims; or (h) Customer-Deployed Model IP claims. If the Software is or may become subject to an infringement claim, Magure may, at its option and expense, (i) procure the right to continue use, (ii) modify the Software to be non-infringing while substantially preserving functionality, or (iii) terminate the affected subscription and refund pre-paid fees for the unused period. This Section states Magure's entire liability and Customer's exclusive remedy for IP infringement claims.

14.2 By Customer. Customer shall defend, indemnify, and hold harmless Magure (and its Affiliates, officers, and personnel) from third-party claims arising from (a) Customer Data (including IP infringement, privacy violations, or unlawful content); (b) Customer's use of Outputs, including decisions or actions taken based on Outputs; (c) breach of Section 6 (Acceptable Use) or Section 12 (AI-Specific Provisions); (d) Customer's combination of the Software with third-party products or services; (e) claims by Customer's end users; or (f) Customer's violation of applicable law.

14.3 Outputs. Given the inherent nature of generative AI and the involvement of third-party Foundation Models, neither Party indemnifies the other for third-party IP claims arising from Outputs, except where Magure expressly commits to such coverage in writing for a specific Output type.

14.4 Procedure. The indemnified Party shall promptly notify the indemnifying Party of the claim, give it sole control of the defence and settlement (provided no settlement imposes liability or obligations on the indemnified Party without consent), and reasonably cooperate at the indemnifying Party's expense.

15. LIMITATION OF LIABILITY

15.1 Liability Cap. EXCEPT FOR THE EXCLUSIONS IN SECTION 15.3, EACH PARTY'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATING TO THIS AGREEMENT SHALL NOT EXCEED THE FEES PAID OR PAYABLE BY CUSTOMER FOR THE SOFTWARE THROUGH AWS MARKETPLACE IN THE SIX (6) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM.

15.2 Indirect Damages. NEITHER PARTY SHALL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES, INCLUDING LOST PROFITS, LOST REVENUE, LOST DATA, BUSINESS INTERRUPTION, OR LOSS OF GOODWILL, EVEN IF ADVISED OF THE POSSIBILITY.

15.3 Exclusions from Cap. The limitations in Sections 15.1 and 15.2 do not apply to: (a) Customer's breach of Section 6 (Acceptable Use) or Section 12 (AI-Specific Provisions); (b) Customer's infringement or misappropriation of Magure's Intellectual Property Rights; (c) either Party's breach of confidentiality (Section 10); (d) Customer's indemnification obligations under Section 14.2; (e) amounts payable for the Software; and (f) a Party's gross negligence, wilful misconduct, or fraud, and any liability that cannot be excluded by law.

15.4 Allocation of Risk. The Parties acknowledge that these limitations are an essential basis of the bargain and a reasonable allocation of risk reflected in the fees.

16. TERM, SUSPENSION, AND TERMINATION

16.1 Term. This Agreement takes effect on Customer's acceptance and continues for the Subscription Term specified in the applicable Order through AWS Marketplace. Unless a different term is specified in the Order, the initial Subscription Term is three (3) years from the subscription start date (the "Initial Term"). After the Initial Term, the subscription renews for successive twelve (12) month Renewal Terms in accordance with the renewal settings of the applicable Order on AWS Marketplace, unless either Party elects not to renew under those settings. This Agreement remains in effect for as long as any subscription is active.

16.2 No Termination for Convenience. Neither Party may terminate this Agreement or any subscription for convenience during the Initial Term, regardless of the Subscription Term selected (12, 24, or 36 months). The Subscription Term is a binding commitment for its full duration, and the fees for the committed Subscription Term remain due and payable notwithstanding any early discontinuation of use by Customer. Except for a termination by Customer for Magure's uncured material breach under Section 16.3 (for which Customer's sole refund remedy is set out in Section 11.2), no refund of prepaid or committed fees is owed on any termination, and all amounts are handled through AWS Marketplace. During any Renewal Term, either Party may elect not to renew by giving notice in accordance with the renewal settings of the applicable Order on AWS Marketplace and, where applicable, at least sixty (60) days before the end of the then-current term.

16.3 Termination for Cause. Either Party may terminate this Agreement or the affected subscription on written notice if the other Party materially breaches and fails to cure within thirty (30) days of notice (or ten (10) days for non-payment), or becomes insolvent. Magure may terminate immediately for Customer's breach of Section 6 (Acceptable Use), Section 8 (Intellectual Property), or Section 10 (Confidentiality).

16.4 Suspension. Magure may suspend Customer's access to the Software (or, in a Self-Hosted Deployment, disable license keys) where Customer's use poses a security, legal, or infringement risk, violates Section 6, or where fees are overdue, with notice where practicable.

16.5 Effect of Termination. On termination or expiry, the licence ends and Customer shall cease using the Software and, in a Self-Hosted Deployment, delete or de-install all copies. Customer's ownership of Customer Data, Customer Build-on Assets, and Outputs is unaffected. In a Hosted Deployment, Magure shall, on written request within thirty (30) days after termination, make Customer Data available for export in a standard machine-readable format, after which Magure may delete it from systems Magure controls. Refunds, if any, are handled through AWS Marketplace and Section 11.2.

16.6 Survival. Sections 1, 5 (as to accrued amounts), 6.2, 8, 10, 11.3, 12, 14, 15, 16.5, 16.6, 17, and 18 survive termination.

17. GOVERNING LAW AND DISPUTE RESOLUTION

17.1 Governing Law. This Agreement is governed by the laws of the Dubai International Financial Centre (DIFC), without reference to conflict-of-law principles. The United Nations Convention on Contracts for the International Sale of Goods does not apply.

17.2 Escalation. The Parties shall first attempt to resolve any dispute by good-faith escalation to senior representatives within thirty (30) days.

17.3 Jurisdiction. Subject to Section 17.4, the courts of the DIFC shall have exclusive jurisdiction to settle any dispute arising out of or in connection with this Agreement. For subscriptions negotiated as a private offer, the Parties may instead agree in that offer to resolve disputes by arbitration administered by the DIFC-LCIA Arbitration Centre (or its successor), seated in the DIFC, in English, before a single arbitrator.

17.4 Injunctive Relief. Either Party may seek injunctive or equitable relief in any court of competent jurisdiction to protect its Intellectual Property Rights or Confidential Information.

18. GENERAL PROVISIONS

18.1 Relationship to AWS / No Reliance by AWS. AWS is not a party to this Agreement, makes no warranties regarding the Software, and has no obligation or liability to Customer under this Agreement. Customer's transactional and billing relationship is governed by the AWS Agreement. To the extent permitted by AWS Marketplace, AWS is an intended third-party beneficiary of the disclaimers and use restrictions in this Agreement solely as they protect AWS.

18.2 Order of Precedence. As between Magure and Customer regarding the Software: a mutually executed private offer or written agreement prevails over this EULA; this EULA prevails over the Documentation. This Agreement does not amend the AWS Agreement.

18.3 No Additional Terms. Customer acknowledges that any conflicting or additional terms in a purchase order or similar Customer document have no effect.

18.4 Export Control and Sanctions. Customer shall comply with all applicable export control and sanctions laws (including those of the UAE, the United States, the EU, and the UK) and shall not use or export the Software in violation of such laws, or make it available to any sanctioned or restricted person or territory.

18.5 Anti-Corruption. Each Party shall comply with applicable anti-corruption laws, including the UAE laws, the U.S. Foreign Corrupt Practices Act, and the UK Bribery Act.

18.6 U.S. Government End Users. The Software is a "commercial product" / "commercial computer software" and is provided to U.S. Government end users with only those rights granted to all other end users under this Agreement.

18.7 Assignment. Customer may not assign this Agreement without Magure's prior written consent, except to a successor in connection with a merger, acquisition, or sale of substantially all assets, on prior written notice and provided the assignee is not a Magure competitor and assumes this Agreement. Magure may assign to an Affiliate or successor.

18.8 Subcontracting. Magure may use subcontractors and subprocessors to perform its obligations, remaining responsible for their performance.

18.9 Force Majeure. Neither Party is liable for any delay or failure (except payment obligations) caused by events beyond its reasonable control, including acts of God, war, terrorism, civil unrest, government action, internet or utility failures, pandemics, or failures of Foundation Model providers, cloud infrastructure providers, or AWS.

18.10 Independent Contractors. The Parties are independent contractors; nothing creates a partnership, agency, joint venture, or employment relationship.

18.11 Publicity. Neither Party shall use the other's name, logo, or trademarks without prior written consent, except that Magure may identify Customer as a customer in customer lists with Customer's prior approval (not unreasonably withheld).

18.12 Updates to this EULA. Magure may update this EULA for new subscriptions and renewals by posting an updated version on the AWS Marketplace listing. The version in effect when Customer subscribes or renews governs that Subscription Term.

18.13 Notices. Legal notices to Magure shall be sent to: Magure Tech Middle East Ltd, Attn: Legal & Compliance, Unit 195, Level 1, Gate Avenue – South Zone, DIFC, Dubai, UAE; email: legal@magureinc.com. Notices to Customer may be sent to the contact or account information associated with Customer's AWS Marketplace subscription.

18.14 Severability; Waiver; Cumulative Remedies. If any provision is unenforceable, the remainder remains in effect and the provision is reformed to the minimum extent necessary. Failure to enforce is not a waiver. Remedies are cumulative.

18.15 Entire Agreement. This Agreement (together with any applicable private offer, DPA, and the Documentation) is the entire agreement between the Parties regarding the Software and supersedes all prior or contemporaneous understandings on that subject matter.

© 2026 Magure Tech Middle East Ltd. All rights reserved.

ANNEX A — DATA PROCESSING ADDENDUM

MagOneAI – AWS Marketplace

This Data Processing Addendum (“DPA”) forms part of, and is incorporated into, the End User License Agreement for MagOneAI (AWS Marketplace) between Magure Tech Middle East Ltd (“Magure”) and the customer that subscribes to the Software through AWS Marketplace (“Customer”) (the “Agreement” or “EULA”). Capitalised terms not defined here have the meanings given in the EULA. This DPA applies only to the extent Magure Processes Personal Data on Customer’s behalf in connection with the Software.

1. Definitions

1.1 “Data Protection Laws” means all data protection and privacy laws applicable to a Party’s Processing of Personal Data under the Agreement, including, as applicable, the EU General Data Protection Regulation 2016/679 (“GDPR”), the UK GDPR and Data Protection Act 2018, the UAE Federal Decree-Law No. 45 of 2021 (PDPL), the DIFC Data Protection Law No. 5 of 2020, the ADGM Data Protection Regulations 2021, and any other applicable law governing the protection of Personal Data.

1.2 “Controller”, “Processor”, “Data Subject”, “Processing”, “Personal Data Breach”, and “Supervisory Authority” have the meanings given in the GDPR (or the equivalent concepts under other applicable Data Protection Laws).

1.3 “Customer Personal Data” means Personal Data contained within Customer Data that Magure Processes on Customer’s behalf under the Agreement.

1.4 “SCCs” means the Standard Contractual Clauses approved by the European Commission in Implementing Decision (EU) 2021/914.

1.5 “UK Addendum” means the UK International Data Transfer Addendum to the SCCs issued by the UK Information Commissioner.

2. Roles and Scope

2.1 Roles. As between the Parties, Customer is the Controller (or a Processor acting on behalf of a third-party controller) of Customer Personal Data, and Magure is the Processor. Where Customer is itself a Processor, Magure is a sub-processor and Customer warrants it has the controller’s authority to engage Magure on these terms.

2.2 Self-Hosted Deployments. Customer acknowledges that, in a Self-Hosted Deployment, Customer Personal Data resides at all times within the Customer Cloud Environment under Customer’s control and is not transmitted to or stored by Magure. In such deployments Magure does not Process Customer Personal Data except to the limited, Customer-instructed extent described in Section 2.3, and this DPA applies only to that limited Processing.

2.3 Scope of Processing. Magure Processes Customer Personal Data only (a) in a Hosted Deployment, to host and operate the Software as a service; and (b) in either deployment, to the limited extent Customer instructs Magure to provide scoped support, troubleshooting, or Professional Services requiring access to Customer Personal Data. Details of the Processing are set out in Annex I.

2.4 Magure Not a Controller. Magure is not the Controller, joint Controller, or independent Controller of Customer Personal Data. Magure may Process aggregated and anonymised operational metrics that do not identify any Data Subject as a Controller for its own legitimate security, performance, and service-improvement purposes, consistent with Section 8.4 of the EULA.

3. Customer Obligations

3.1 Customer shall comply with its obligations as Controller under Data Protection Laws, including establishing a lawful basis for Processing, providing all required notices to Data Subjects, and obtaining all necessary consents.

3.2 Customer's instructions to Magure for the Processing of Customer Personal Data shall comply with Data Protection Laws. Customer is solely responsible for the accuracy, quality, and legality of Customer Personal Data and the means by which it acquired it.

3.3 Customer is responsible for configuring the Software's access, retention, and security controls appropriately for the sensitivity of Customer Personal Data, including classification of any special-category, health, financial, or children's data.

4. Magure Obligations

Magure shall, with respect to Customer Personal Data it Processes on Customer's behalf:

4.1 Instructions. Process Customer Personal Data only on Customer's documented instructions (including those set out in the Agreement and this DPA), unless required to do otherwise by applicable law, in which case Magure shall, where legally permitted, inform Customer of that legal requirement before Processing.

4.2 Confidentiality. Ensure that personnel authorised to Process Customer Personal Data are bound by appropriate confidentiality obligations.

4.3 Security. Implement and maintain the technical and organisational measures set out in Annex II, consistent with Magure's ISO 27001-certified information security management system and ISO 42001-aligned AI governance system, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and risk of the Processing.

4.4 Assistance. Taking into account the nature of the Processing, provide reasonable assistance to Customer (insofar as possible) in fulfilling Customer's obligations to respond to Data Subject rights requests and to carry out data protection impact assessments and prior consultations with Supervisory Authorities. Magure may charge a reasonable fee for assistance beyond standard Software functionality.

4.5 Breach Notification. Notify Customer without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach affecting Customer Personal Data within Magure's control, and provide information reasonably available to assist Customer in meeting its breach-notification obligations.

4.6 Deletion or Return. On termination or expiry of the Agreement, delete or return Customer Personal Data in accordance with Section 16.5 of the EULA and Section 9 of this DPA, except where retention is required by applicable law.

4.7 Records and Compliance. Make available to Customer information reasonably necessary to demonstrate compliance with this DPA, as further described in Section 7.

5. Sub-Processors

5.1 General Authorisation. Customer provides general authorisation for Magure to engage sub-processors to Process Customer Personal Data, subject to this Section. A current list of sub-processors is set out in Annex III.

5.2 Flow-Down. Magure shall impose data protection obligations on each sub-processor that are no less protective than those in this DPA, and remains liable to Customer for the acts and omissions of its sub-processors.

5.3 Changes. Magure shall give Customer reasonable prior notice (by the means stated in Annex III) of the addition or replacement of a sub-processor. Customer may object on reasonable, data-protection-related grounds within fourteen (14) days; the Parties shall work in good faith to resolve the objection, and if unresolved, Customer's sole remedy is to terminate the affected subscription with the refund (if any) determined under the EULA.

6. International Transfers

6.1 Primary Safeguard – Data Residency. The Parties acknowledge that MagOneAI's design keeps Customer Personal Data within the Customer-designated environment, minimising international transfers. In a Self-Hosted Deployment, Customer determines the location of all Processing.

6.2 Transfer Mechanisms. To the extent Magure's Processing of Customer Personal Data involves a transfer subject to Chapter V of the GDPR or an equivalent cross-border transfer restriction, and no other lawful transfer mechanism applies, the following are incorporated by reference and apply: (a) the SCCs (Module Two, Controller-to-Processor, or Module Three, Processor-to-Processor, as applicable), with Magure as data importer and Customer as data exporter; and (b) for transfers subject to UK law, the UK Addendum. The Annexes to the SCCs are populated by Annexes I–III of this DPA, and the option for general sub-processor authorisation (with the notice period in Section 5.3) applies.

6.3 UAE / DIFC. For transfers subject to UAE PDPL or DIFC Data Protection Law, the Parties shall rely on the adequacy, standard contractual clause, or other transfer mechanisms recognised under those laws, and shall execute any additional documentation reasonably required.

6.4 Conflict. Where the SCCs apply, and there is a conflict between the SCCs and this DPA or the EULA, the SCCs prevail with respect to the transfer they govern.

7. Audits

7.1 Magure shall make available to Customer, on reasonable written request and no more than once per twelve (12) months (unless required by a Supervisory Authority or following a Personal Data Breach), Magure's then-current third-party audit reports and certifications (e.g., ISO 27001) and a completed security questionnaire, as evidence of compliance.

7.2 Where such information is insufficient to demonstrate compliance with this DPA, Customer (or its mandated auditor, bound by confidentiality, and not a Magure competitor) may conduct an audit on at least thirty (30) days' written notice, during business hours, without unreasonably disrupting Magure's operations, at Customer's cost, and subject to Magure's security and confidentiality requirements.

8. Liability

8.1 Each Party's liability arising out of or related to this DPA, whether in contract, tort, or otherwise, is subject to the limitations and exclusions of liability set out in Section 15 of the EULA, and any reference in the EULA to the "Agreement" includes this DPA. The Parties' total aggregate liability under the EULA and this DPA together shall not exceed the cap in Section 15.1 of the EULA.

9. Deletion and Return

9.1 On termination or expiry of the Agreement, Magure shall, at Customer's election made within thirty (30) days, delete or make available for export Customer Personal Data Processed on Customer's behalf, in accordance with Section 16.5 of the EULA, after which Magure shall delete remaining copies within its control, save where retention is required by applicable law (in which case this DPA continues to apply to such retained data).

10. General

10.1 Order of Precedence. In the event of a conflict, the SCCs prevail (as to the transfers they govern), then this DPA (as to data protection matters), then the EULA. In all other respects the EULA continues in full force.

10.2 Governing Law. This DPA is governed by the law of the DIFC and subject to the dispute-resolution provisions of Section 17 of the EULA, except where Data Protection Laws or the SCCs mandate otherwise for the Processing or transfer they govern.

10.3 Changes in Law. If a change in Data Protection Laws requires amendment of this DPA, the Parties shall negotiate in good faith to make the minimum necessary changes; Magure may post an updated DPA in accordance with Section 18.12 of the EULA.

Annex I — Description of Processing

Subject matter	Provision of the MagOneAI Software (Hosted Deployment) and scoped support / Professional Services.
Duration	The Subscription Term and any post-termination export/deletion window.
Nature & purpose	Hosting, operating, supporting, and maintaining the Software; troubleshooting; delivery of Professional Services on Customer's instructions.
Types of Personal Data	As determined and submitted by Customer through Customer Data; may include identifiers, contact data, professional data, and any data Customer ingests into knowledge bases or agent inputs. Customer controls whether special categories are submitted.
Categories of Data Subjects	As determined by Customer (e.g., Customer's employees, contractors, end users/customers).
Controller	Customer (or the third-party controller Customer represents).
Processor	Magure Tech Middle East Ltd.

Annex II — Technical and Organisational Measures

Magure maintains controls consistent with ISO 27001 and ISO 42001, including: information security policies and governance; access control on a least-privilege, role-based basis with multi-factor authentication for administrative access; encryption of Personal Data in transit and, where Magure stores it, at rest; secure software development lifecycle and change management; logging, monitoring, and audit trails; vulnerability and patch management; personnel screening and confidentiality obligations; security-awareness training; incident detection and response with the notification commitment in Section 4.5; business continuity and backup for systems Magure controls; and vendor/sub-processor security due diligence. In a Self-Hosted Deployment, security of the Customer Cloud Environment is Customer's responsibility per Section 9.3 of the EULA.

Annex III — Sub-Processors

Notice of changes is provided to the Customer's registered subscription contact by email and/or via a subscriber portal. Objection window: fourteen (14) days (Section 5.3). Self-Hosted Deployments without Magure support access involve no Magure sub-processors, as Customer Personal Data remains in the Customer Cloud Environment.

Sub-processor	Purpose	Location	Applies to
Amazon Web Services, Inc.	Cloud hosting infrastructure for Hosted Deployment	Any AWS region selected by Customer	Hosted Deployment only
Atlassian (Jira)	Customer support case management	Germany	Hosted and Self-Hosted (support access)

