END USER LICENSE AGREEMENT
BASTION PROMPT PROTECTION

Vendor: Bastionsoft UAB, a company organized under the laws of Lithuania, company registration number 307761630 ("Vendor"). **Licensee:** the legal entity identified on the order form or invoice ("Licensee"). **Effective Date:** the date of the first invoice issued by Vendor to Licensee for the commercial license.

This Agreement governs Licensee's use of the commercial version of the Model. The AGPL-licensed variant of the xsmall English model is governed solely by the GNU Affero General Public License v3.0 and is outside the scope of this Agreement.

1. DEFINITIONS

Model. The fine-tuned prompt-injection-detection model artifact made available by Vendor under this Agreement, in any size or language variant, together with associated configuration files.

Licensed Artifact. The specific copy of the Model delivered to Licensee, including any embedded fingerprint identifying Licensee.

Update. Any new version, revision, or successor of the Model released by Vendor during the License Period.

Documentation. The user documentation, code samples, and microservice templates published by Vendor at https://docs.bastionsoft.com

Output. Any classification, score, label, or other inference result produced by the Model in response to an input.

Product. A single, branded software product offered by Licensee, regardless of the number of tenants, regions, or replicas in which it operates.

Production Environment. An environment in which the Model processes inputs originating from end users of a Product.

Non-Customer-Facing Environment. A development, test, staging, UAT, or disaster-recovery environment that is not directly accessed by end users, including those that process production-like data.

Affiliate. An entity that directly or indirectly owns, is owned by, or is under common ownership with another entity, where ownership means holding more than 50% of voting rights or equity.

Group. Licensee and its Affiliates, taken together.

Competitor. Any entity whose business meaningfully includes the development, distribution, or commercialization of prompt-injection-detection models, AI safety classifiers, or substantially similar AI security products.

2. LICENSE GRANT

Subject to Licensee's continued compliance with this Agreement and payment of the applicable fees, Vendor grants Licensee a non-exclusive, non-transferable, non-sublicensable right, during the License Period, to:

(a) install and use the Licensed Artifact within Licensee's own infrastructure, or the infrastructure of a cloud provider acting on Licensee's behalf, for the purposes permitted by the applicable License Tier;

(b) fine-tune or further train the Model for Licensee's own internal use, subject to Section 4;

(c) make a reasonable number of backup and archival copies of the Licensed Artifact;

(d) generate and use Outputs in connection with Licensee's Products.

All other rights are reserved by Vendor.

3. LICENSE TIERS

3.1 Team/Product Tier — EUR 3,999 per annum

One Product, in one Production Environment, plus up to five Non-Customer-Facing Environments. The Product may operate across multiple regions, replicas, and high-availability or disaster-recovery configurations.

3.2 Company Tier — EUR 15,999 per annum

One legal entity, in one country of invoicing, covering up to twenty Products and up to one hundred Non-Customer-Facing Environments. Multi-brand and white-labelled products operated by the same legal entity are permitted within this Tier. The Licensee may service customers in multiple jurisdictions provided that all customer invoicing is issued by a single legal entity.

3.3 Enterprise Tier — Custom Pricing

The Company Tier extended to all Affiliates within the Group. Acquisitions completed during the License Period are absorbed into the Tier without additional fees until the next renewal, subject to Section 16.

3.4 Tier Mechanics

Licensee may upgrade to a higher Tier at any time. On upgrade, Vendor credits Licensee the pro-rata unused portion of the prior Tier's fees against the new Tier's fees, and a new twelve (12) month Initial Term for the new Tier begins on the upgrade date.

Licensee shall self-report any growth that causes its use to exceed the limits of its then-current Tier within 30 days, and shall either purchase additional licenses of the same Tier or upgrade.

The change of the single invoicing entity referenced in Section 3.2 is permitted on prior written notice to Vendor.

4. RESTRICTIONS

Licensee shall not:

(a) distribute, redistribute, publish, share, or otherwise make available the Model, its weights, or any portion of either, to any third party, including via container registries, model hubs, file shares, or backups outside Licensee's control;

(b) embed or include the Model or its weights in any software, container image, or other artifact provided to any third party, including end users of Licensee's Products;

(c) operate or host any service whose principal commercial purpose is to make Model inference available to third parties, whether for free or for consideration; this restriction does not prevent Licensee from using the Model as an internal component of its own Products and surfacing decisions, classifications, or other information derived from Outputs to its end users, provided that the Model, its weights, and its inference endpoint themselves are not made directly accessible to those end users;

(d) resell, rent, lease, sublicense, or otherwise commercialize the Model, or operate the Model on behalf of any third party as a managed service or outsourced offering, without a separate written agreement with Vendor;

(e) use Outputs to train, fine-tune, distill, evaluate-for-training, or otherwise develop any model intended to perform prompt-injection detection or a substantially similar task;

(f) reverse engineer the Model's weights, attempt to extract the training data, or remove, obscure, or circumvent any fingerprint, watermark, identifier, or notice embedded in or accompanying the Licensed Artifact;

(g) remove or alter the copyright notices, third-party license notices (including the MIT license notice for the upstream Microsoft DeBERTa model), or other proprietary markings included with the Licensed Artifact.

5. UPDATES

Vendor will make all Updates released during the License Period available to Licensee at no additional cost, announced by email to Licensee's designated contact and on Vendor's website. Vendor is not obligated to maintain backward compatibility and may deprecate or discontinue any variant of the Model.

6. LICENSEE ASSISTANCE

Vendor provides a designated email address through which Licensee may report (i) suspected defects in the Model relative to the Documentation, (ii) errors in the Documentation, and (iii) questions regarding the published code samples. Vendor will use commercially reasonable efforts to acknowledge such reports but makes no commitment as to response time, resolution time, or any particular outcome. No service-level agreement applies. Licensee Assistance does not include assistance with Licensee's deployment, infrastructure, integrations, training, fine-tuning, or other matters not arising directly from defects in the Model or the Documentation. Vendor may, at its discretion, offer paid support packages under separate written agreement.

7. FEES, TAXES, AND PAYMENT

Fees are stated in euros (EUR) and are payable via Stripe in accordance with the invoice schedule.

Fees are exclusive of all taxes, duties, and similar governmental charges. Licensee shall pay or reimburse Vendor for all such taxes, excluding only taxes on Vendor's net income. For Licensees established in the European Union and providing a valid VAT identification number, the reverse charge mechanism applies where available. For Licensees established outside the European Union, fees are invoiced without EU VAT on the basis that the supply is outside the scope of EU VAT as a B2B supply of services. Where any withholding tax is required by law, Licensee shall gross up the payment such that Vendor receives the full invoiced amount.

Licensee's obligation to pay accrued fees is not subject to any limitation of liability under this Agreement.

8. TERM AND TERMINATION

8.1 TERM

This Agreement begins on the Effective Date and continues for an initial term of twelve (12) months ("Initial Term"). After the Initial Term, this Agreement continues automatically on a month-to-month basis

("Renewal Period") until terminated under this Section. The Initial Term and any Renewal Period together are the "License Period".

8.2 FEES AND RENEWAL

Fees for the Initial Term are payable in advance. During any Renewal Period, fees are charged monthly in advance at one-twelfth (1/12) of the then-current annual fee for Licensee's Tier. Vendor may adjust the monthly fee for a future Renewal Period on 30 days' prior written notice.

8.3 TERMINATION FOR CONVENIENCE

Either party may terminate this Agreement at the end of the Initial Term, or at the end of any subsequent monthly Renewal Period, on at least 30 days' written notice. Termination for convenience does not entitle Licensee to a refund of fees already paid for the then-current period.

8.4 TERMINATION FOR CAUSE

Vendor may terminate this Agreement on written notice if Licensee materially breaches the Agreement and fails to cure within 30 days of written notice, or immediately for breach of Section 4 (Restrictions), Section 15 (Confidentiality), Section 17 (Acceptable Use), or Section 20 (Export Control and Sanctions). Termination does not relieve Licensee of accrued payment obligations.

8.5 EFFECT OF TERMINATION

On expiry or termination of this Agreement for any reason, all licenses granted under Section 2 end immediately. Licensee shall, within 30 days, cease all use of the Model, permanently delete all copies of the Licensed Artifact, the Model, its weights, and any backups or derivatives in Licensee's possession or control, and, on Vendor's request, certify such deletion in writing by an authorized officer. Outputs generated and retained by Licensee before termination are not subject to this deletion obligation.

9. OUTPUTS

As between the parties, Licensee owns the Outputs generated by its use of the Model. Outputs are probabilistic and are provided subject to the disclaimers in Section 11. A determination by the Model that an input is or is not a prompt injection is not a security guarantee, and Licensee is responsible for the use it makes of any Output.

10. BENCHMARK STATEMENT

Vendor publishes benchmark results for the Model at https://docs.bastionsoft.com, reproducible using Vendor's published scripts on the public datasets identified in the Documentation. If a headline benchmark figure for Licensee's licensed Model version is shown to deviate from reproducible measurement by more than five (5) percentage points on the published dataset, methodology, and Model version, and Licensee notifies Vendor in writing within 12 months of Licensee's first download of that Model version, Vendor shall, within 60 days of notice, at its option: (i) correct the published benchmark; (ii) release an Update that closes the gap; or (iii) refund the fees paid for the then-current Initial Term or, during a Renewal Period, the fees paid for the preceding twelve (12) months. This refund is Licensee's sole and exclusive remedy for any inaccuracy in published benchmark figures.

Variations within the threshold above reflect the probabilistic nature of the Model and do not constitute a breach. The benchmark statement concerns measurement on the specific public datasets identified by Vendor and does not constitute a warranty as to Model performance on Licensee's data or use cases.

11. DISCLAIMER OF WARRANTIES

Except for the benchmark statement in Section 10 and the indemnity in Section 12, the Model, Documentation, and any other materials provided by Vendor are provided "as is" and "as available", without warranties of any kind, whether express, implied, or statutory, including warranties of merchantability, fitness for a particular purpose, non-infringement, accuracy, completeness, or uninterrupted operation.

Licensee acknowledges that (i) the Model is probabilistic and will produce false positives and false negatives; (ii) the Model is one defense layer and is not a substitute for defense-in-depth security controls; and (iii) Vendor makes no commitment as to detection accuracy on Licensee's inputs or in Licensee's environment.

12. VENDOR INDEMNIFICATION

Vendor shall defend Licensee against any third-party claim that the Model, in the form delivered by Vendor and used in accordance with this Agreement, infringes the third party's copyright, trade secret, or registered patent in Licensee's jurisdiction, and shall pay damages and reasonable costs finally awarded by a court of competent jurisdiction or agreed in settlement.

This indemnity is conditioned on Licensee (i) notifying Vendor in writing within 30 days of becoming aware of the claim, (ii) granting Vendor sole control of the defense and settlement, and (iii) providing reasonable cooperation at Vendor's expense.

This indemnity does not apply to claims arising from (a) modifications, fine-tuning, or further training of the Model by or for Licensee; (b) combination of the Model with software, data, weights, or systems not provided by Vendor; (c) use of the Model in breach of this Agreement; (d) continued use of a Model version after Vendor has made a non-infringing Update available; (e) use of any Model version more than 12 months after a successor version was released; or (f) the inputs Licensee processes through the Model or Licensee's use of Outputs.

On a covered claim, Vendor may, at its option: (i) procure for Licensee the right to continue using the Model; (ii) modify the Model so as to be non-infringing while substantially preserving functionality; or (iii) terminate the license and refund the pro-rata unused portion of fees paid. This is Licensee's sole and exclusive remedy for any claim of infringement by the Model.

Vendor's total liability under this Section is capped at two (2) times the fees paid by Licensee to Vendor in the 12 months preceding the claim.

13. LICENSEE INDEMNIFICATION

Licensee shall defend Vendor and its Affiliates against any third-party claim arising from (a) Licensee's breach of Section 4 (Restrictions) or the license grant; (b) the inputs Licensee processes through the Model; (c) Licensee's use of Outputs, including any downstream product, decision, or representation made on the basis of Outputs; (d) Licensee's modifications, fine-tuning, or combination of the Model with other software; (e) Licensee's breach of Section 17 (Acceptable Use), Section 20 (Export Control and Sanctions), or applicable law. Licensee shall pay damages and reasonable costs finally awarded by a court of competent jurisdiction or agreed in settlement. This indemnity is not subject to the limitation of liability in Section 14.

14. LIMITATION OF LIABILITY

Except as provided in this Section, each party's aggregate liability under or in connection with this Agreement shall not exceed the fees paid by Licensee to Vendor in the 12 months preceding the event giving rise to the liability. Neither party shall be liable for indirect, consequential, special, incidental, exemplary, or punitive damages, or for lost profits, lost revenue, lost data, or reputational harm, regardless of the form of action.

The cap and the exclusion of indirect damages above do not apply to: (i) Licensee's breach of Section 4 (Restrictions), Section 15 (Confidentiality), Section 17 (Acceptable Use), or Section 20 (Export Control and Sanctions); (ii) either party's indemnification obligations, which are governed by Sections 12 and 13 respectively; (iii) Licensee's obligation to pay accrued fees; or (iv) liability that cannot be limited under applicable law, including liability for gross negligence, willful misconduct, fraud, death, or personal injury.

15. CONFIDENTIALITY

Each party shall protect the other party's confidential information with the same degree of care it uses for its own confidential information, and in no event less than reasonable care, and shall use it only for the purposes of this Agreement. The Model, its weights, and the Licensed Artifact are Vendor's confidential information regardless of whether marked as such. Confidentiality obligations survive for three (3) years after termination, except that trade secrets remain confidential for as long as they retain trade-secret status.

16. WATERMARKING AND ANTI-PIRACY

Vendor may embed in each Licensed Artifact a passive, statistical fingerprint that uniquely identifies the copy delivered to Licensee. The fingerprint does not transmit, log, or otherwise communicate any information at any time and is purely passive. Its sole purpose is to enable Vendor to identify the source of any unauthorized copy of the Model that Vendor may encounter outside Licensee's authorized deployment. Licensee shall not remove, obscure, or attempt to remove the fingerprint, and acknowledges that any unauthorized copy of the Model is identifiable as having originated from the Licensee's Licensed Artifact.

On Vendor's written notice citing a specific concern, Licensee shall provide reasonable cooperation with Vendor's investigation of suspected unauthorized distribution, including confirming the fingerprint of copies deployed within Licensee's environment and identifying the locations of authorized deployments. This is not a right of audit.

Licensee shall self-report any use that exceeds the limits of its License Tier in accordance with Section 3.4.

17. ACCEPTABLE USE

Licensee shall not use the Model:

(a) for any practice prohibited under Article 5 of Regulation (EU) 2024/1689 (the EU AI Act);

(b) to produce, distribute, or detect child sexual abuse material other than for the purpose of detection by qualified entities authorized under applicable law;

(c) to support the design, development, or operation of weapons or weapons-targeting systems;

(d) to conduct unlawful surveillance of individuals;

(e) to attack, disrupt, or gain unauthorized access to any system operated by Vendor or its Affiliates;

(f) in violation of applicable law.

Vendor may terminate this Agreement immediately on written notice if Licensee breaches this Section.

18. NO TELEMETRY; DATA PROTECTION

The Model is designed for fully offline operation. The Model does not transmit, during installation or inference, any data, telemetry, usage metrics, configuration information, or other information to Vendor or any third party. The Model may be operated in fully air-gapped environments without loss of functionality.

Vendor does not collect personal data, customer data, or operational data from Licensee's use of the Model. Vendor is not a processor of personal data within the meaning of applicable data protection law with respect to Licensee's use of the Model, and no data processing agreement is required.

19. EU AI ACT ALLOCATION

The Model is a task-specific AI component provided by Vendor to Licensee. Vendor's obligations as a provider of the Model under the EU AI Act are limited to those that apply to the Model as delivered.

Licensee is solely responsible for determining whether its use of the Model brings any of its AI systems within the scope of the EU AI Act, and for fulfilling all obligations of a provider, deployer, importer, or distributor of such systems, including conformity assessment, risk management, post-market monitoring, registration, human oversight, transparency, and instructions for use.

On Licensee's reasonable written request, Vendor will provide the technical information about the Model reasonably necessary for Licensee to discharge its own obligations under Article 25 of the EU AI Act, limited to performance metrics, intended purpose, known limitations, instructions for use, and training data categories at a level of generality consistent with Vendor's trade-secret protections. Vendor's cooperation obligation does not extend to bespoke documentation, customer-specific assessments, or assistance with Licensee's conformity dossier.

Licensee shall not represent that the Model has been assessed for conformity in respect of any specific high-risk use, or that Vendor has approved any specific use case.

20. EXPORT CONTROL AND SANCTIONS

Licensee represents that it is not, and is not owned or controlled by, a person or entity subject to applicable export control or sanctions restrictions, and is not located in a sanctioned territory. Licensee shall not export, re-export, transfer, or make the Model available to any such person, entity, or territory. Vendor may terminate this Agreement immediately if compliance with this Section becomes impracticable.

21. ASSIGNMENT AND CHANGE OF CONTROL

Vendor may assign this Agreement in connection with a merger, acquisition, reorganization, or sale of all or substantially all of Vendor's assets or business to which this Agreement relates, without Licensee's consent.

Licensee shall not assign this Agreement, including by operation of law, merger, change of control, or asset sale, to a Competitor without Vendor's prior written consent. Assignment to any non-Competitor does not require Vendor's consent.

Licensee shall notify Vendor in writing within 30 days of any change of control affecting Licensee. If Licensee undergoes a change of control to a Competitor, Vendor may terminate this Agreement on 30 days' written notice, with pro-rata refund of unused prepaid fees.

22. REFERENCE AND PUBLICITY

Neither party shall use the other party's name, logo, or trademarks in marketing, press, customer lists, or case studies without the other party's prior written consent on a per-use basis. Vendor may include Licensee in aggregate, non-identifying customer counts and statistics, and may disclose the existence of the commercial relationship to actual or prospective investors, acquirers, and professional advisors under reasonable confidentiality obligations.

23. RELATIONSHIP TO AGPL VARIANT

An AGPL-3.0-licensed variant of the xsmall English-language Model is available for research and evaluation purposes. This Agreement is independent of and not derived from that license. The network-use copyleft and other obligations of the AGPL do not apply to the commercial Licensed Artifact delivered under this Agreement. Licensee shall not commingle AGPL-licensed and commercial artifacts in the same deployment.

24. GENERAL

Governing law. This Agreement is governed by the laws of the Republic of Lithuania, excluding conflict-of-laws rules and the UN Convention on Contracts for the International Sale of Goods.

Forum. The courts of Vilnius, Lithuania have exclusive jurisdiction over disputes arising out of or in connection with this Agreement.

Language. The English-language version of this Agreement is the controlling version.

Notices. Notices to Vendor shall be sent to info@bastionsoft.com. Notices to Licensee shall be sent to the contact identified on the order form. Notices are effective on receipt.

Force majeure. Neither party is liable for failure or delay in performance caused by events beyond its reasonable control, excluding payment obligations.

Entire agreement. This Agreement, together with the order form and the Documentation, is the entire agreement between the parties on its subject matter and supersedes any prior or contemporaneous understandings. Any order-form term that conflicts with this Agreement is superseded except where the order form expressly states that it overrides a specifically identified Section.

Severability. If any provision is held unenforceable, the remainder of this Agreement remains in effect, and the unenforceable provision shall be modified to the minimum extent necessary to make it enforceable while preserving the parties' original intent.

No waiver. Failure to enforce any provision is not a waiver of the right to enforce it later.

Independent contractors. The parties are independent contractors. Nothing in this Agreement creates a partnership, agency, joint venture, or employment relationship.

Survival. Sections 4, 7 (with respect to accrued fees), 8.5, 9, 11, 12, 13, 14, 15, 16, 19, 20, 22, 23, and 24 survive termination.