ENTERPRISE CUSTOMER AGREEMENT

This Enterprise Customer Agreement (this "**Agreement**") is entered into by and between the customer identified in the signature block below or in the Order under GSA Schedule Contract as as applicable ("**Customer**") and AIQ Phase LLC dba xAI organized under the laws of the State of Wyoming ("**xAI**") (Customer and xAI each, a "**party**" and collectively, the "**parties**"), effective as of the date of the last signature below ("**Effective Date**"), and sets forth the terms and conditions under which Customer may subscribe to certain products and services of xAI as set forth in one or more order forms or other ordering documents executed by the parties that reference this Agreement (each, an "**Order Form**").

Accepted and agreed to as of the Effective Date by the authorized representative of each party:

CUSTOMER:	**XAI:** Address: 1450 Page Mill Rd. Palo Alto, CA 94304
Signature	Signature
Name	Name
Title	Title
Date Signed	Date Signed
Email:	Email: support@x.ai

1. XAI PRODUCTS AND SERVICES

1.1. Provision of Products and Services. Subject to the terms and conditions of this Agreement, xAI will provide Customer with the online software-as-a-service products and services on a subscription basis for the Subscription Term (defined below), and such other products and services, as set forth on an applicable Order Form (collectively, the "**Service(s)**"). Each Order Form will be incorporated into, and is fully governed by, this Agreement upon execution of the Order Form by both parties. In the event of any conflict or inconsistency between this Agreement and an Order Form, this Agreement shall control, unless expressly stated otherwise in the Order Form.

1.2. Access to Services. Customer may access and use the Services on a non-exclusive and non-transferrable basis (except as set forth in Section 1.4), solely for its business purposes as specified herein and the applicable Order Form, and only in accordance with the terms and conditions of this Agreement, the applicable Order Form, and any technical documentation provided by xAI for such Services currently available at https://docs.x.ai/docs (as may be updated from time to time) ("**Documentation**"). Subject to this Agreement, xAI grants Customer a limited, non-exclusive right to use xAI's application programming interfaces to develop an integration between the Services and Customer's products (the "**Bundled Services**") and to: (a) make available the Bundled Service to Customer's end users ("**End-Users**"); and (b) demonstrate the Bundled Services to potential End-Users. Customer will provide access to the Services to End-Users only in accordance with this Agreement. This grant does not create any direct contractual relationship between xAI and the End-Users. Customer shall remain responsible to xAI for each End-User. If the Order Form permits Customer's End-Users to develop an integration between the Services and their own products (each an "**Additional Bundled Service**"), then all references to End-Users in this Agreement will mean both End-Users and Additional Bundled Service end users.

1.3. Permitted Users. Customer may permit its employees, agents, independent contractors and consultants to use the Services solely on its behalf ("**Permitted Users**"), provided Customer remains responsible for the acts and omissions of each such Permitted User. Use of the Services by Customer in the aggregate must be within the restrictions set forth in the applicable Order Form (if any). If Customer is given passwords to access Services on xAI's systems, Customer shall require that all Permitted Users keep user ID and password information strictly confidential and not share such information with any unauthorized person. Customer shall promptly notify xAI: (a) if Customer has reason to suspect that any user ID or password has been lost, stolen, compromised, or misused, and (b) of any unauthorized access to or use of the Services. Customer shall be responsible for any and all actions taken by Customer or its Permitted Users in the Customer's accounts and passwords.

1.4. Use by Affiliates. Each of Customer's Affiliates (defined below) identified on an Order Form will be entitled to access and use the applicable Services in accordance with this Agreement and the applicable Order Form; provided that Customer shall remain responsible to xAI for the actions and omissions of each such Affiliate (and each of such Affiliate's Permitted Users). The terms of this Agreement will govern, and will be incorporated by reference into, each such Order Form as if this Agreement were separately executed by the applicable Customer Affiliate, and the term "Customer" as used in this Agreement will be deemed as applying to such Customer Affiliate for the purposes of such Order Form. "**Affiliate**" means an entity that, directly or indirectly, controls, is controlled by, or is under common control with a party. As used herein, "control" means the power to direct the management or affairs of an entity or the beneficial ownership of fifty percent (50%) or more of the voting equity securities or other equivalent voting interests of an entity.

1.5. Beta Offerings. From time to time, xAI may, in its sole discretion, include test features or products in the Services ("**Beta Offerings**"). If Customer chooses to use any Beta Offerings, Customer agrees such offerings are provided "as is" and may contain errors, defects, bugs or inaccuracies that could fail or cause corruption or loss of data and information. Customer agrees that use of any Beta Offerings is at its own risk. If xAI provides Customer with access to non-public Beta Offerings, Customer agrees that they are offered on a confidential basis and are xAI Confidential Information and the use of such Beta Offerings by Customer may be governed and controlled by separate terms outside of this Agreement. Separate terms outside this Agreement governing Customer's use of such Beta Offerings shall be provided to the cognizant GSA Contracting Officer for review and incorporation into the terms and conditions of applicable GSA Contract.

2. General Restrictions. Customer shall comply with xAI's Acceptable Use Policy (**"AUP"**) currently available at https://x.ai/legal/acceptable-use-policy and attached hereto as Exhibit #1 (as it may be non-materially updated from time to time in accordance with GSAR Clause 552.212-4(w)(1)(vi)). Further, Customer shall not, and shall not allow any third party (including any Permitted User) to: (a) sell, rent, lease or use any xAI Service for time sharing purposes; (b) use any xAI Service to help develop, or help provide to any third party, any product or service similar to or competitive with any xAI Service, unless expressly approved in the Order Form (and for the avoidance of doubt, this subclause (b) shall not prohibit End-Users accessing the Services pursuant to a license stated in Section 1 hereto); (c) reverse engineer, decompile, disassemble, or otherwise seek to obtain the source code of any xAI Service; (d) copy, modify or create derivative works from any xAI Service or any Documentation; (e) scrape any User Content, distill model behavior, or remove or obscure any copyright or proprietary or other notice contained in any xAI Service or Documentation; (f) propagate any virus, Trojan horse, or other malware or programming routine intended to damage any system or data; (g) access or use any Services in a manner intended to circumvent or exceed service account limitations or requirements; (h) use any Services in a manner that violates any applicable law, regulation, or legal requirement or obligation; (i) use any Services in violation of any third-party rights of privacy or intellectual property rights; (j) use or permit the use of any tools in order to probe, scan or attempt to penetrate or benchmark any Services; (k) post, upload, transmit or provide any Input (defined below) or other data that xAI reasonably deems to be unlawful, harmful, abusive or otherwise violates this Agreement (l) use the Services except as expressly permitted by this Agreement. Customer shall ensure that its agreements with End-Users will contain an acceptable use policy, terms and conditions, and a privacy policy that are substantially consistent with, and at least as protective of Customer and xAI as, this Agreement, the AUP, and xAI's Privacy Policy. If xAI or Customer reasonably suspects a breach of this Section resulting from the activity of its End-Users, it shall promptly notify the other party in writing. Upon such notice, the parties agree to cooperate in good faith to investigate and address the suspected breach. This may include, to the extent legally permissible, taking corrective measures, such as temporarily suspending or terminating the account of any End-User found to be in violation of the terms of this Agreement in accordance with the contract Disputes Clause (Contract Disputes Act).

3. CUSTOMER OBLIGATIONS; DATA

3.1. Generally. "**Input**" means information, data, and other content, in any form or medium, that is downloaded, or otherwise received, directly or indirectly (including via a third-party provider), from Customer (including from a Permitted User on Customer's behalf) or any End-User to xAI to be processed by the Services. Input does not include information, data, or other content submitted by Customer to xAI outside of the Services, including non-production data and synthetic

data. As between the parties, Customer is solely responsible for the accuracy, content and legality of all Input uploaded by the Customer or any End-User. Customer represents and warrants to xAI that Customer has sufficient rights in the Input and has obtained all required consents to grant the rights granted to xAI in Section 3.2 below and that the Input to the Customer's knowledge does not infringe or otherwise violate the rights of any third party.

3.2. Rights in Input. As between the parties, Customer shall retain all right, title and interest (including any and all intellectual property rights) in and to the Input. Customer hereby grants to xAI a non-exclusive, worldwide, revocable (upon reasonable advance written notice), transferable (as set forth in Section 13.1) fully paid-up, royalty-free right and license to use, copy store, transmit, modify, and display the Input in order to: (a) provide the Services to Customer; and (b) perform such other actions as authorized or instructed by Customer in writing (email to suffice). The use of Government data for the purpose of training artificial intelligence/machine learning models and systems is prohibited without explicit written authorization from the ordering activity contracting officer. Government data means any information, (including metadata), document, media, or machine-readable material regardless of physical form or characteristics that is created or obtained by the Government, or a contractor on behalf of the Government, in the course of official Government business.

3.3. De-identified Data and Data Retention. xAI may create and use de-identified data related to Customer's use of the Services to improve xAI's products and services, to develop new products and services, and for its other business purposes (and such de-identified data will be owned by xAI). For clarity, subject to Section 3.2(a), xAI shall not use any Inputs or Outputs **("User Content")** for any of its internal AI or other training purposes (such as training its machine learning models), including developing new products or services based on User Content. All User Content is automatically deleted within 30 days, unless (a) otherwise agreed in an Order Form, (b) xAI is legally required to retain it, or (c) it is flagged as potentially violating this Agreement or the AUP.

3.4. Output. As between Customer and xAI, Customer owns the output of the Services provided to Customer based on Input ("**Output**"). Customer shall not represent that Output was human-generated or use the Output to train Customer's or its providers' machine learning models. Due to the nature of machine learning, the Output may not be unique across users and the xAI Service may generate the same or similar Output for other users. Use of the xAI Service may result in incorrect Output that does not accurately reflect reality. Customer must evaluate the accuracy of any Output as appropriate for Customer's use case, including by using human review of the Output. xAI does not warrant the accuracy of Output. If Customer shares Input or Output from the xAI Service with others, Customer authorizes xAI to share those materials with the applicable third party. Customer is responsible for complying with relevant third-party policies when it instructs xAI to transmit Output to those third parties.

3.5. Third-Party Application Service Providers. Customer may be able to access and use certain optional third-party services or products (e.g., a third-party service that integrates with xAI via opt-in, or uses xAI's APIs) through or with its use of the Services ("**Third-Party Services**"). Customer is under no obligation to use any Third-Party Services. Additionally, all or some portions of the Services may be subject to additional and/or separate terms and conditions, including but not limited to open-source software licenses and other third-party software license terms and conditions ("**Third-Party Terms**"). Other than open-source software licenses, nothing herein shall bind the Ordering Activity to any Third-Party Terms unless the terms are provided for review and agreed to in writing by all parties. To the extent there is a conflict between the Third-Party Terms and this Agreement, the Third-Party Terms and conditions shall control. NOTWITHSTANDING ANYTHING IN THIS AGREEMENT TO THE CONTRARY, ALL THIRD-PARTY SERVICES ARE MADE AVAILABLE ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND. IF CUSTOMER USES ANY THIRD-PARTY SERVICES, XAI WILL NOT BE RESPONSIBLE FOR ANY ACT OR OMISSION OF ANY PROVIDER OF SUCH THIRD-PARTY SERVICES. XAI DOES NOT WARRANT OR PROVIDE DIRECT SUPPORT FOR ANY THIRD-PARTY SERVICES. CUSTOMER ACKNOWLEDGES AND AGREES THAT XAI WILL HAVE NO RESPONSIBILITY OR LIABILITY FOR THE ACTS OR OMISSIONS OF ANY PERMITTED USERS IN CONNECTION WITH ANY THIRD-PARTY SERVICES.

4. OWNERSHIP

4.1. Ownership. Customer acknowledges that no intellectual property rights are assigned or transferred to Customer hereunder. Customer is obtaining only a limited right to access and use the Services set forth on the applicable Order Form. Customer agrees that xAI or its suppliers own and retain all right, title and interest (including all patent, copyright, trade secret and other intellectual property rights) in and to (a) the Services, Documentation, and any and all related and underlying technology, documentation, and other information, (b) any intellectual property it develops hereunder, and any derivatives thereof, and (c) all improvements or modifications to the foregoing (a) and (b) ((a), (b) and (c) individually and collectively, "**xAI Technology**"). As between xAI and Customer, Customer owns all right, title and interest in and to the Output in perpetuity and, to the fullest extent possible under applicable law, xAI hereby assigns to Customer all of its right, title, and interest in and to such Output (but excluding, for clarity, any xAI Technology).

4.2. Feedback. In the event Customer or any Permitted User provides xAI with any suggestions, ideas,

improvements or other feedback with respect to any aspect of the Services ("**Feedback**"), Customer hereby assigns and shall cause all Permitted Users to assign to xAI all right, title and interest in and to such Feedback, including all intellectual property rights therein, and acknowledges that xAI shall own such Feedback. xAI acknowledges that the ability to use this Agreement and any Feedback provided as a result of this Agreement in advertising is limited by GSAR 552.203-71

5. SUBSCRIPTION TERM, FEES AND PAYMENT

5.1. Subscription Term and Renewals. Unless otherwise terminated as set forth below, each Order Form will have a term as set forth therein (the **"Initial Term"**). Thereafter, each Order Form will renew by mutual agreement of the parties for successive renewal terms of equal length to the Initial Term (each, a **"Renewal Term,"** and together with the Initial Term, the **"Subscription Term"**). If no term is stated on an Order Form, the Subscription Term for such Order Form is one (1) year.

5.2. Fees and Payment. All fees are as set forth in the applicable Order Form in accordance with the GSA Schedule Pricelist and shall be paid by Customer within thirty (30) days of xAI's invoice receipt date, unless otherwise specified in the applicable Order Form. Except as otherwise set forth in the applicable Order Form, all fees are due and at the start of the applicable Subscription Term (and each Renewal Term). Fees are payable by credit card, check, or through ACH transfers. Upon xAI's request, Customer agrees to promptly complete and submit an ACH authorization form to xAI. xAI shall state separately on invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the equipment) or provide evidence necessary to sustain an exemption, in accordance with 552.212-4(k).

5.3. Suspension of Service. xAI also reserves the right to temporarily suspend Customer's access to the Services immediately if Customer's use of the Services: (a) reserved; (b) raises suspicion of fraud, misuse, security concern, illegal activity or unauthorized access issues; or (c) to protect the integrity or availability of the Services or xAI's systems.

6. TERM AND TERMINATION

6.1. Term. This Agreement is effective as of the Effective Date and will continue in effect until terminated as set forth below.

6.2. Termination.. When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, xAI shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

6.3. Effect of Termination. Upon the expiration or termination of this Agreement, (a) Customer shall immediately cease all use of and access to the Services (including any and all related xAI Technology) and (b) each party will return to the other party (or destroy) such other party's Confidential Information (defined below) within 30 days. Except as otherwise set forth herein, termination of this Agreement is not an exclusive remedy and the exercise by either party of any remedy under this Agreement will be without prejudice to any other remedies it may have under this Agreement, by law, or otherwise.

6.4. Survival. The following Sections shall survive any expiration or termination of this Agreement: 1.4, 2, 3, 4, 5, 6.2, 6.3, 7, 8, 9, 10, 11, and 13.

7. LIMITED WARRANTY; DISCLAIMER

7.1. Limited Warranty. Each party represents and warrants to the other that it has the full right and power to enter into and perform under this Agreement, without any third party consents or conflicts with any other agreement. xAI warrants that it will provide the Services in substantial conformity with the applicable Documentation and the descriptions in the Order Form. xAI's sole liability (and Customer's sole and exclusive remedy) for any breach of this warranty shall be, in xAI's sole discretion and at no charge to Customer, to use commercially reasonable efforts to provide Customer with an error correction or work-around that corrects the reported non-conformity, or if xAI determines such remedies to be impracticable, to allow Customer to terminate the Subscription Term and receive as its sole and exclusive remedy and xAI's entire liability, a refund of any fees Customer has pre-paid for use of the Services or related services it has not received as of the date of the warranty claim. The limited warranty set forth in this Section shall not apply: (a) if the error was caused by the Bundled Services, Additional Bundled Services, or any misuse, unauthorized modifications or third-party hardware, software or services, or (b) to any Services provided on a no-charge or evaluation basis.

7.2. Warranty Disclaimer. EXCEPT FOR THE WARRANTIES SET FORTH IN THIS AGREEMENT, THE SERVICES ARE PROVIDED ON AN "AS IS" AND "AS AVAILABLE" BASIS. XAI AND ITS SUPPLIERS EACH EXPRESSLY DISCLAIM ANY OTHER WARRANTIES, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, TITLE, OR FITNESS FOR A PARTICULAR PURPOSE.

8. LIMITATION OF LIABILITY

8.1. Exclusion of Damages. NEITHER PARTY SHALL BE LIABLE, UNDER ANY LEGAL OR EQUITABLE THEORY OF LAW, WITH RESPECT TO ANY SUBJECT MATTER OF THIS AGREEMENT FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL OR PUNITIVE DAMAGES OF ANY KIND, INCLUDING LOST PROFITS, BUSINESS, CONTRACTS, REVENUE, GOODWILL, PRODUCTION, AND ANTICIPATED

SAVINGS OR DATA, EVEN IF INFORMED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO (1) PERSONAL INJURY OR DEATH RESULTING FROM LICENSOR'S NEGLIGENCE; (2) FOR FRAUD; OR (3) FOR ANY OTHER MATTER FOR WHICH LIABILITY CANNOT BE EXCLUDED BY LAW.

8.2. Limitation of Liability. EXCEPT WITH RESPECT TO EITHER PARTY'S OBLIGATIONS IN SECTION 2 (GENERAL RESTRICTIONS), SECTION 9 (INDEMNIFICATION) OR SECTION 10 (CONFIDENTIAL INFORMATION), EITHER PARTY'S OBLIGATIONS REGARDING THE OTHER PARTY'S PROPRIETARY RIGHTS, EITHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, OR CUSTOMER'S PAYMENT OBLIGATIONS, EACH PARTY'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT, WHETHER IN CONTRACT, TORT OR OTHERWISE, SHALL IN NO EVENT EXCEED THE FEES PAID BY CUSTOMER TO XAI DURING THE TWELVE (12) MONTH PERIOD PRIOR TO WHEN THE CLAIM AROSE.

9. INDEMNIFICATION

9.1. Indemnification by xAI. xAI shall indemnify and have the right to intervene to defend Customer from and against any claims, costs, damages, losses, liabilities and expenses (including reasonable outside attorneys' fees and costs) arising from infringement of patent, copyright, trademark, or other intellectual property right asserted against Customer by a third party based upon Customer's use of the Services in accordance with the terms of this Agreement; provided that xAI shall have received from Customer: (a) prompt written notice of such claim; (b) the right to control and direct the investigation, defense, or settlement (if applicable) of such claim (as long as such settlement releases Customer from any and all liability); and (c) all reasonable necessary cooperation of Customer at xAI's expense. Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516. In addition, Customer may, at its own cost and expense, appoint its own counsel with respect to defense of the claim; and any settlement that does not provide for a full and unconditional release of Customer shall require Customer's consent. If Customer's use of any xAI Service is, or in xAI's opinion is likely to be, enjoined due to the type of infringement specified above, or if required by settlement, xAI may, in its sole and reasonable discretion: (x) substitute substantially functionally similar products or services; (y) procure for Customer the right to continue using the Services; or if (x) and (y) are commercially impracticable, (z) terminate this Agreement and refund to Customer any unused, prepaid fees paid by Customer for the terminated period. The foregoing indemnification obligation of xAI shall not apply to the extent that the alleged infringement arises from: (1) any modification of the Services, including fine-tuning or other customization, other than by or on behalf of xAI; (2) access to or use of any xAI Service in combination with any hardware, system, software, network, or other products, materials or services not provided by or on behalf of xAI, including the Bundled Services; (3) use of the Services in breach of this Agreement, including the AUP, Documentation, DPA, and xAI Privacy Policy; or (4) Input, Output, or any training data Customer provides to xAI, if any. THIS SECTION 9.1 SETS FORTH XAI'S SOLE LIABILITY AND CUSTOMER'S SOLE AND EXCLUSIVE REMEDY WITH RESPECT TO ANY CLAIM OF INTELLECTUAL PROPERTY INFRINGEMENT.

9.2. Reserved .

10. CONFIDENTIAL INFORMATION

10.1. Definition. "**Confidential Information**" means information disclosed by one party to the other that is marked as confidential or proprietary or that ought reasonably to be understood as confidential or proprietary. All xAI Technology, performance information relating to the Services, and the terms and conditions of this Agreement (excluding the fees and pricing information if made publicly available) shall be deemed Confidential Information of xAI without any marking or further designation. Customer's Confidential Information includes User Content (subject to Section 3.4). Confidential Information does not include information that the recipient already lawfully knew, that becomes public through no fault of the recipient, that was independently developed by the recipient without any reference to or use of Confidential Information, or that was rightfully obtained by the recipient from a third party. xAI recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as "confidential" by the vendor, unless an applicable Exemption as defined by the Freedom of Information Act would be reasonably applicable.

10.2. Obligations. The recipient agrees not to disclose Confidential Information except to its Affiliates, employees, contractors and agents who need to know it and have agreed in writing to keep it confidential. Only those parties may use the Confidential Information, and only to exercise the recipient's rights and fulfill its obligations under this Agreement, while using at least a reasonable degree of care to protect it. The recipient may also disclose Confidential Information to the extent required by law after providing reasonable notice to the discloser and cooperating to obtain confidential treatment. Unauthorized disclosure of Confidential Information may cause harm not compensable by damages, and the disclosing party, to the extent applicable or legally permissible, may seek injunctive or equitable relief in a court of competent jurisdiction, without posting a bond, to protect its Confidential Information.

11. PRIVACY; SECURITY

11.1. Privacy. By using the Services, Customer acknowledges that information, including Feedback, relating to individuals associated with Customer and End-User accounts, may be processed as set forth in the xAI Privacy Policy located at https://x.ai/legal/privacy-policy, and attached hereto as Exhibit #2, for reference purposes only, as it may be updated from time to time. Customer acknowledges that if Customer or End-Users incidentally submit it to the Services, xAI may collect, use, and disclose Customer and End-User data which may include "personal data" or "personal information" (as those terms are defined under applicable privacy laws), in which case xAI's Data Processing Addendum ("**DPA**"), attached hereto as **Addendum 1** and incorporated herein by reference, shall apply. In addition, Customer agrees that it shall not submit, and shall prohibit End-Users from submitting to the Services: (a) large or routine volumes of personal data or personal information, (b) any information that includes or constitutes sensitive personal data under any applicable privacy laws or other rules, (c) "protected health information," as defined under the HIPAA Privacy Rule (45 C.F.R. Section 160.103) or (d) financial data, such as data subject to Payment Card Industry Data Security Standard (PCI DSS) requirements. If Customer wishes to process such data, then xAI's Zero Data Retention Addendum ("**ZDR Addendum**"), and Business Associate Agreement ("**BAA**") shall be attached hereto and incorporated herein as **Addendum 2** and **Addendum 3**, respectively, as applicable. Customer shall ensure that use of the Services and Customer and End-User User Content shall always comply with Customer privacy policies and all applicable local, state, federal and international laws, regulations and conventions, including, without limitation, those related to data privacy, international communications, and the exportation of technical or personal information.

11.2. Security. xAI shall use reasonable physical, technical, and administrative procedures designed to protect, safeguard and help prevent loss, misuse, and unauthorized access, disclosure, alteration or destruction of User Content, as described at https://x.ai/security and Appendix 2 of the DPA, and xAI will reasonably choose these safeguards in line with industry standards and based on the sensitivity of the information that is collected, processed, and stored, and the current state of applicable technology.

12. PUBLICITY

Except as otherwise agreed in writing (email to suffice), neither party may use the other's name or marks without the other party's written pre-approval in each case to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71.

13. GENERAL TERMS

13.1. Assignment. This Agreement will bind and inure to the benefit of each party's permitted successors and assigns. Neither party may assign this Agreement or any of its right or obligations hereunder except upon the advance written consent of the other party, except xAI may assign this Agreement and all of its rights and obligations hereunder to an xAI U.S. Affiliate or to a xAI successor entity in connection with a merger, reorganization, acquisition or other transfer of all or substantially all of such party's assets or voting securities in accordance with the provisions set forth at FAR 42.1204 (individually and collectively, an "Approved Assignment"). Any such Approved Assignment will not extend to third-parties separate from xAI Affiliates. Any attempt to transfer or assign this Agreement except as expressly authorized under this Section will be null and void.

13.2. Force Majeure. In accordance with GSAR Clause 552.212-4(f), Neither party shall be liable to the other for any delay or failure to perform any obligation under this Agreement (except for a failure to pay fees) if the delay or failure is due to unforeseen events which occur after the signing of this Agreement and which are beyond the reasonable control of such party, such as a strike, blockade, war, act of terrorism, riot, natural disaster, epidemic, pandemic, government act or failure, or failure or diminishment of power or telecommunications or data networks or services.

13.3. Subcontractors. xAI may use the services of subcontractors for performance of services under this Agreement, provided that xAI remains responsible for the acts and omissions of its subcontractors and such subcontractors' compliance with the terms of this Agreement, including any acts or omissions that, if taken (or not taken) by xAI, would constitute a breach of the Agreement.

13.4. Independent Contractors. The parties to this Agreement are independent contractors. There is no relationship of partnership, joint venture, employment, franchise or agency created hereby between the parties. Neither party will have the power to bind the other or incur obligations on the other party's behalf without the other party's prior written consent.

13.5. Severability. If any provision of this Agreement shall be adjudged by any court of competent jurisdiction to be unenforceable or invalid, that provision shall be limited to the minimum extent necessary so that this Agreement shall otherwise remain in effect.

13.6. Governing Law; Jurisdiction and Venue. This Agreement shall be governed by the laws of the State of Texas without regard to conflict of laws principles. The exclusive venue for any judicial action arising out of or relating to this Agreement will be the state and federal courts in Tarrant County, Texas, and the parties hereby irrevocably consent to the exclusive jurisdiction and venue of such courts.

13.7. Notice. Any notice or communication required or permitted under this Agreement shall be in writing to the parties at the addresses set forth as first listed above or at such other address as may be given in writing by either party to the other in accordance with this Section

and shall be deemed to have been received by the addressee (a) if given by hand, immediately upon receipt; (b) if given by overnight courier service, the first business day following dispatch or (c) if given by registered or certified mail, postage prepaid and return receipt requested, the second business day after such notice is deposited in the mail. In addition, any legal notices to xAI must be delivered to the following email address: legal@x.ai but, notwithstanding earlier receipt via email, legal notices will be deemed received when the physical notice is received (as set forth in preceding sentence).

13.8. Amendments; Waivers. No supplement, modification, or amendment of this Agreement shall be binding, unless executed in writing by a duly authorized representative of each party to this Agreement. No waiver will be implied from conduct or failure to enforce or exercise rights under this Agreement, nor will any waiver be effective unless in a writing signed by a duly authorized representative on behalf of the party claimed to have waived. Purchase orders (and similar documents) issued by Customer are for administrative purposes only (e.g. setting forth products and services ordered and associated fees) and any additional or different terms or conditions contained in any such order shall not apply (even if the order is accepted, or performed on by xAI).

13.9. No Third-Party Rights. There are no third-party beneficiaries to this Agreement.

13.10. Export Compliance. Each party shall comply with all applicable export and re-export control and trade and economic sanctions laws, including the Export Administration Regulations, trade and economic sanctions, and the International Traffic in Arms Regulations. Neither party, nor any of its subsidiaries or any person acting on its behalf or owning 50% or more of its equity securities or other equivalent voting interests, is (a) a person on the List of Specially Designated Nationals and Blocked Persons or any other list of sanctioned persons administered by OFAC or any other governmental entity, or (b) a national or resident of, or a segment of the government of, any country or territory for which the United States has embargoed goods or imposed trade sanctions.

13.11. Entire Agreement. This Agreement is the complete and exclusive statement of the mutual understanding of the parties, and supersedes and cancels all previous written and oral agreements and communications, relating to the subject matter of this Agreement. This Agreement may be executed electronically and in counterparts, which counterparts taken together shall form one legal instrument. Any pre-printed terms in a Customer purchase order or similar document are null and void.

ADDENDUM 1

DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Appendices (the "**DPA**"), entered into by and between X.AI LLC ("**xAI**") and the customer identified in the Enterprise Customer Agreement and/or Test Agreement (the **"Agreement"**) ("**Customer**" or "**you**") (each, a "**party**" and collectively, the "**parties**"), effective as of the date of the last signature in the Agreement ("**Effective Date**"), sets out the terms that apply when xAI processes Personal Data (as defined below) on your behalf in connection with the Service, including any Personal Data that you provide to xAI through our API or other business services.

You enter into this DPA on behalf of yourself and, to the extent required under Applicable Data Protection Laws, in the name and on behalf of your Affiliates permitted to use the Service under the Agreement. If and to the extent the terms of this DPA conflict with the terms of the Agreement, the terms of this DPA shall control. Unless otherwise defined herein, capitalized terms used in this DPA have the same meaning given to them under the Agreement.

If the Customer is performing an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal or State law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is not in accordance with the Federal or State law of the United States.

The Parties agree as follows:

1. Definitions

(a) "**Applicable Data Protection Laws**" means all data protection and privacy laws and regulations applicable to the processing of Personal Data, which may include European Data Protection Laws and U.S. Privacy Laws.

(b) "**Europe**" means the European Economic Area and its Member States, Switzerland, and the United Kingdom ("**UK**").

(c) "**European Data Protection Laws**" means all data protection and privacy laws and regulations of Europe, as applicable to the processing of Personal Data, including (i) the General Data Protection Regulation 2016/679 ("**GDPR**"); (ii) the GDPR as it forms part of UK law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 and the Data Protection Act 2018 (together, "**UK GDPR**"); and (iii) the Swiss Federal Act on Data Protection Act of 2020 and its Ordinance ("**Swiss FADP**"); as may be amended, superseded, or replaced.

(d) "**Personal Data**" means any information defined as "personal information" under the CCPA, "personal data" under the GDPR, or other similar terms under Applicable Data Protection Laws, that you provide to xAI in connection with the Service as User Content and that we process on your behalf, as described in Appendix 1.

(e) "**Restricted Transfer**" means a transfer of Personal Data originating from Europe to a country that does not provide an adequate level of protection for personal data within the meaning of applicable European Data Protection Laws.

(f) "**Security Incident**" means a breach of xAI's or its Subprocessors' security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data in connection with the Service. Security Incidents do not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

(g) "**SCCs**" means the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021, as may be amended, superseded, or replaced.

(h) "**Subprocessor**" means any third-party processor engaged by xAI to process Personal Data in order to provide the Service. Subprocessors do not include xAI's employees, contractors, or consultants.

(i) "**UK Addendum**" means the International Data Transfer Addendum issued by the UK Information Commissioner under Section 119A of the Data Protection Act 2018, as may be amended, superseded, or replaced.

(j) "**U.S. Privacy Laws**" means all federal and state data protection and privacy laws and regulations of the United States, as applicable to the processing of Personal Data, including (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act (Cal. Civ. Code §§ 1798.100 et seq.), and its implementing regulations ("**CCPA**"); (ii) the Virginia Consumer Data Protection Act (VA Code Ann. §§ 59.1-575 et seq.) ("**VCDPA**"); (iii) the Colorado Privacy Act (Colo. Rev. Stat. §§ 6-1-1301 et seq.) and its implementing regulations ("**CPA**"); (iv) the Connecticut Data Privacy Act (Pub. Act No. 22015) ("**CTDPA**"); and (v) the Utah Consumer Privacy Act (Utah Code Ann. §§ 13-61-101 et seq.) ("**UCPA**"); in each case when effective and as may be amended, superseded, or replaced.

(k) The terms "**controller**", "**data subject**", "**personal data**", "**process**", "**processing**", "**processor**", and "**supervisory authority**" have the meanings given to them under Applicable Data Protection Laws.

2. Processing of Personal Data

2.1 **Scope and Roles.** This DPA applies to the extent that we process Personal Data on your behalf in connection with the provision of the Service under the Agreement. The parties acknowledge and agree that xAI is a processor and you are a controller or processor of Personal Data, as applicable, under Applicable Data Protection Laws.

2.2 **Details of Processing.** The subject matter, duration, nature, and purpose of the processing of Personal Data, and the types of Personal Data and categories of data subjects, are described in Appendix 1.

2.3 **Your Responsibilities.** You shall, in your use of the Service:

(a) comply with your obligations under Applicable Data Protection Laws, including (i) ensuring that your processing instructions to xAI comply with Applicable Data Protection Laws; and (ii) obtaining all necessary rights, consents, and authorizations required to provide Personal Data to xAI and allow us to process Personal Data as contemplated by the Agreement;

(b) without prejudice to our security obligations under Section 5.1 (Security Measures), use the Service in a secure manner, including by (i) securing your account authentication credentials; (ii) ensuring the security of systems and devices used to access the Service; and (iii) backing up or retaining copies of Personal Data as appropriate; and

(c) if you are a processor of Personal Data, (i) warrant that the relevant controller has authorized your engagement of xAI as another processor and approved your processing instructions to us; and (ii) remain responsible for any communications, notifications, assistance, and/or authorizations that may be required in connection with the processing of Personal Data.

2.4 **xAI's Responsibilities.** We shall comply with our obligations under Applicable Data Protection Laws in our role as a processor and inform you if we cannot or can no longer meet such obligations. As a processor, we agree to:

(a) process Personal Data solely in accordance with your lawful and documented processing instructions, where such instructions are consistent with the terms of the Agreement;

(b) inform you if, in our reasonable opinion, your processing instructions infringe Applicable Data Protection

Laws;

(c) if Personal Data is subject to U.S. Privacy Laws, not (i) "sell" or "share" Customer Personal Data (as defined by the CCPA or equivalent concepts under U.S. Privacy Laws); (ii) retain, use, disclose, or otherwise process Personal Data outside of our direct business relationship; or (iii) combine Personal Data with Personal Data collected or received from or on behalf of any third party; except to the extent necessary to provide the Service; and

(d) if you permit or instruct us to process Personal Data in a deidentified, anonymized, and/or aggregated form, (i) adopt reasonable measures to prevent such information from being used to infer information about, or otherwise being linked to, a particular data subject; (ii) not attempt to reidentify such information except to determine that the information has been effectively deidentified in accordance with Applicable Data Protection Laws; and (iii) contractually obligate any recipients of such information to comply with the requirements of this provision.

2.5 **No Assessment of Compliance.** Notwithstanding the foregoing, xAI is not responsible for monitoring your compliance with applicable laws or determining if your processing instructions are compliant with applicable laws. Furthermore, we have no obligation to assess Personal Data in order to identify information that is subject to specific legal requirements.

3. Subprocessors

3.1 **Appointment of Subprocessors**. You agree and provide a general written authorization that xAI may engage Subprocessors to process Personal Data. xAI's list of general Subprocessors is available here ("**Subprocessor List**"). xAI shall (a) enter into a written agreement with each Subprocessor containing data protection obligations that are substantially the same as those in this DPA; and (b) remain liable for any acts or omissions of our Subprocessors that causes us to breach our obligations under this DPA.

3.2 **Changes to Subprocessors.** xAI will notify you if we add or replace Subprocessors at least fifteen (15) days before such changes take effect. You may object on reasonable grounds relating to data protection to our engagement of any new or replacement Subprocessor by informing us in writing within fifteen (15) days after receiving notice. Such notice shall explain the reasonable grounds for the objection. The parties shall discuss the objections in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, xAI will, at its sole discretion, either not appoint the Subprocessor or permit you to terminate the affected part of the Service in accordance with the termination provisions under the Agreement without liability to either party (but without prejudice to any fees incurred by you prior to such termination). This termination right is your sole and exclusive remedy if you object to any new or replacement Subprocessor. If you do not exercise your right to object in the terms defined above, your silence shall be deemed to constitute an approval of such engagement.

4. Confidentiality

4.1 **Confidentiality.** We shall ensure that any persons authorized to process Personal Data are subject to a duty of confidentiality that survives the termination of their employment and/or contractual relationship.

4.2 **Government Requests.** We shall not disclose Personal Data to any law enforcement agency or government authority (collectively, "**Government Authority**") unless instructed by you or as necessary to comply with applicable laws or a valid and binding order of a Government Authority, such as a subpoena or court order. If a Government Authority requests access to Personal Data, and unless legally prohibited from doing so, we shall (a) inform the Government Authority that xAI is a processor and attempt to redirect the Government Authority to you (and we may provide your basic contact information to the Government Authority for such purposes); or (b) in the event such redirection is not possible, notify you of the request to allow you to seek a protective order or other appropriate remedy. If we are legally compelled to respond to the request, we shall review the legality of the request and determine whether the request may be challenged. In any event, we shall only disclose the

minimum information required to comply with the request.

5. Security

5.1 **Security Measures.** We shall implement and maintain reasonable commercially available technical and organizational measures, as appropriate to the processing of Personal Data, that are designed to protect the security, confidentiality, integrity and availability of Personal Data and protect against Security Incidents, as further described in Appendix 2 ("**Security Measures**"). We may update or modify the Security Measures from time to time provided that such updates and modifications do not decrease the overall security of the Service.

5.2 **Audits and Security Certifications**. Upon written request, and subject to reasonable notice and confidentiality agreements, we will provide access to documentation that adequately demonstrates our compliance with this DPA, including copies of certifications, audit reports, and/or other relevant documentation. At our discretion, we may instead make available a summary of the results of third-party certifications and/or audits relevant to our compliance with this DPA.

5.3 **Incident Notification.** We will notify you without undue delay, and where feasible, no later than 48 hours, after we become aware of any Security Incident. Such notification will describe the nature of the Security Incident and include other relevant information that we are reasonably able to disclose, taking into account the nature of the Service, the information available to us, and any restrictions on disclosing the information (such as confidentiality). Any notification that we provide relating to Security Incidents shall not be construed as an acknowledgement by xAI of any fault or liability.

5.4 Any notification required under this Section is meant to satisfy the requirements under Applicable Data Protection Law and include, where legally required, information that can be ascertained with reasonable commercially available technology and effort, such as: (i) a description of the Security Incident, including the number and categories of individuals affected, categories and number of records concerned, types of Personal Data affected, likely consequences of the Security Incident, and date and time of such incident; (ii) a summary of the incident that caused the Security Incident and any ongoing risks that the Security Incident poses; (iii) the name and contact information of the individual who can provide more information to Customer; (iv) a description of the likely consequences of the Security Incident; (v) a description of the measures proposed or taken by xAI to address the Security Incident; (vi) any other information required under Applicable Data Protection Law or reasonably requested by Customer. If and solely to the extent it is not possible to provide the above information at the same time, the information may be provided in phases without undue delay. In the event of a Security Incident, Customer has the right to control the breach notification process including, but not limited to, control over notifying any individuals, regulators, and supervisory authorities, or third parties of the Security Incident, unless Applicable Data Protection Law dictates otherwise.

6. Data Subject Rights Requests

6.1 To the extent required under Applicable Data Protection Laws and taking into account the nature of the Service, and insofar as you cannot respond using functionality made available through the Service, we shall provide you with reasonable assistance to enable you to respond to requests from data subjects seeking to exercise their rights under Applicable Data Protection Laws. In the event that we receive such requests from data subjects directly, we will promptly notify you and not respond directly to the data subject without your prior written authorization, except to inform the data subject that we are a processor and direct them to contact you.

7. Data Protection Impact Assessments

7.1 Upon written request, and to the extent required under Applicable Data Protection Laws, we shall, considering the nature of the processing and the information available to xAI, provide you with reasonable cooperation and assistance necessary to fulfill your obligation to carry out data protection impact assessments and consult with supervisory authorities related to your use of the Service. We shall comply with the foregoing by (i) complying

with Section 5.2 (Audits and Security Certifications); (ii) providing the information contained in the Agreement (including this DPA); or (iii) upon request, if the information provided under sub-sections (i) and (ii) is insufficient for you to fulfill such obligations, providing additional reasonable cooperation and assistance.

8. International Data Transfers

8.1 **International Data Transfers.** You acknowledge and agree that xAI may transfer and process Personal Data outside Europe as necessary to provide the Service, including the United States and other countries where xAI and its Subprocessors maintain data processing operations. We shall take all such measures as are necessary to ensure such transfers are made in compliance with Applicable Data Protection Laws and this DPA.

8.2 **Standard Contractual Clauses.** To the extent that your transfer of Personal Data to xAI involves a Restricted Transfer, the SCCs shall be incorporated and form an integral part of the DPA as follows:

(a) EU Transfers. In relation to Personal Data that is subject to the GDPR: (i) Module Two (Controller to Processor) or Module Three (Processor to Processor) shall apply, as applicable; (ii) in Clause 7, the optional docking clause shall apply; (iii) in Clause 9, Option 2 shall apply and the time period for prior notice of Subprocessor changes is set out in Section 3.2) Changes to Subprocessors); (iv) in Clause 11, the optional language shall not apply; (v) in Clause 17, Option 1 shall apply and the SCCs shall be governed by the laws of the Republic of Ireland; (vi) in Clause 18(b), disputes shall be resolved before the courts of the Republic of Ireland; and (vii) Annexes I and II of the SCCs shall be deemed completed with the information set out in Appendices 1 and 2 of this DPA respectively.

(b) UK Transfers. In relation to Personal Data that is subject to the UK GDPR, the SCCs shall apply in accordance with Section 8.2(a) (EU Transfers) and as modified by the UK Addendum, which shall be deemed executed by the parties and incorporated into and form an integral part of this DPA. Any conflict between the SCCs and the UK Addendum shall be resolved in accordance with Sections 10 and 11 of the UK Addendum. Tables 1 to 3 of the UK Addendum shall be deemed completed with the information set out in Appendices 1 and 2 of this DPA respectively, and Table 4 shall be deemed completed by selecting "neither party".

(c) Swiss Transfers. In relation to Personal Data that is subject to the Swiss FADP, the SCCs shall apply in accordance with Section 8.2(a) (EU Transfers) and the following modifications: (i) references to "Regulation (EU) 2016/679" and specific articles therein shall be replaced with references to the Swiss FADP and the equivalent articles or sections therein; (ii) references to "EU", "Union" and "Member State" shall be replaced with references to "Switzerland"; (iii) the competent supervisory authority shall be the Swiss Federal Data Protection Information Commissioner; (iv) references to the "competent supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland"; and (v) the SCCs shall be governed by the laws of Switzerland and disputes shall be resolved before the applicable courts of Switzerland.

9. Deletion of Personal Data

9.1 Upon termination of the Agreement, we shall delete any Personal Data in our possession in accordance with the Agreement, except to the extent that we are required to retain copies under applicable laws, in which case we shall isolate and protect such Personal Data from any further processing except to the extent required by applicable laws. For clarity, xAI may continue to process information derived from Personal Data that you have instructed us to deidentify, anonymize, and/or aggregate such that the data is no longer considered personal data under Applicable Data Protection Laws.

10. General Provisions

10.1 **Legal Effect; Term.** This DPA is an addendum to and is incorporated into the Agreement. Except for the changes made by this DPA, the Agreement remains unchanged and in full force and effect. This DPA supersedes and

replaces all prior or contemporaneous representations, understandings, agreements, or communications between the parties, whether written or verbal, regarding the subject matter of this DPA, including any data processing addenda previously entered into between the parties. This DPA shall continue in force until the termination of the Agreement and so long as xAI continues to process Personal Data on your behalf.

10.2 **Limitation of Liability**. The liability of each party under this DPA (including the SCCs) shall be subject to the exclusions and limitations of liability set out in the Agreement. In no event does this DPA restrict or limit the rights of any data subject under Applicable Data Protection Laws.

10.3 **Disclosure of this DPA.** You acknowledge that xAI may disclose this DPA and any relevant privacy provisions of the Agreement to a supervisory authority or other judicial or regulatory body upon request.

10.4 **Governing Law**. This DPA shall be governed by and construed in accordance with the governing law and jurisdiction provisions of the Agreement, unless otherwise required by this DPA or Applicable Data Protection Laws.

Appendix 1: Description of the Processing

This Appendix describes the processing of Personal Data by the parties in connection with the Service and forms an integral part of the Agreement. Unless otherwise defined herein, capitalized terms in this Appendix have the same meaning ascribed to them in the Agreement.

(A) List of parties

Data Exporter:	
Name:	The data exporter is the entity identified as the Customer in the applicable registration documents for the Service.
Address:	The data exporter's address is set out in the applicable registration documents for the Service.
Contact person's name, position, and contact details:	The data exporter's contact information is set out in the applicable registration documents for the Service.
Activities relevant to data transferred under these Clauses:	Processing activities in receiving the Service as set out in the Agreement.
Role (controller / processor):	Controller / Processor

Data Importer:	
Name:	X.AI LLC
Address:	1450 Page Mill Rd. Palo Alto, CA 94304 United States
Contact person's name, position, and contact details:	Head of Legal Legal, xAI 1450 Page Mill Rd. Palo Alto, CA 94304 privacy+enterprise@x.ai
Activities relevant to data transferred under these Clauses:	Processing activities in providing the Service as set out in the Agreement.
Role (controller / processor):	Processor

(B) Description of the transfer

Categories of data subjects:	End users of the data exporter's products, services, or applications that access the Service and whose information is provided to xAI through the xAI API or other business services.

Categories of personal data or personal information:	The information processed through the Service is determined and controlled by the data exporter in its sole discretion. Such information may include Personal Data incidentally included within Inputs (i.e., information actively provided to Grok) and Outputs (i.e., responses generated by Grok).
Sensitive data (if applicable) and applied restrictions or safeguards:	The information processed through the Service is determined and controlled by the data exporter in its sole discretion. Subject to any applicable restrictions and/or conditions in the Agreement, such information may include sensitive data incidentally included within Inputs and Outputs, such as Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life, or data relating to criminal offenses or convictions. See Appendix 2 for applied restrictions and safeguards for sensitive data.
Frequency of the transfer:	Continuous
Nature of the processing:	Collection, storage, organization, modification, retrieval, disclosure, communication, and other processing in performance of the Service as set out in the Agreement.
Purpose(s) and subject matter of the transfer and further processing:	Processing activities in performance of the Service as set out in the Agreement, including accessing Grok via our API.
Period and duration for which the personal data or personal information will be processed and retained:	In accordance with Section 9 (Return and Deletion of Personal Data) of the DPA.
For transfers to (sub-) processors, also specify subject matter, nature, and duration of the processing:	Performance of the Service pursuant to the Agreement.

(C) Competent supervisory authority

For the purposes of the SCCs, the competent supervisory authority shall be determined in accordance with the GDPR.

Appendix 2: Security Measures

This Appendix describes the technical and organizational measures implemented by xAI to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and forms an integral part of the Agreement. Unless otherwise defined herein, capitalized terms in this Appendix have the same meaning ascribed to them in the Agreement.

The following table provides examples of the technical and organizational measures implemented by xAI.

Type of measure	**Description of measure**
Measures of pseudonymisation and	All User Content is de-identified using per customer hashed identifiers, and encrypted at rest and in transit, using industry standard encryption (AES-256 encryption for data at rest

Type of measure	Description of measure
encryption of personal data	and TLS 1.3 for data in transit).
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Access to User Content is restricted to authorized personnel only, and all personnel with access are subject to confidentiality agreements. Background checks are performed (where legally permissible) of employees with access to User Content. Employees are subject to annual security training. Access to User Content and any identifying information is further restricted through the use of hash based pseudonymisation. Technical controls are in place to restrict access to data and systems based on job functions and authority levels (e.g., in accordance with “least privilege” and "need-to-know" principles, use of unique identities for each user, enforcement of password complexity requirements, revocation of access upon termination or change in job function). Regular reviews of user access rights are performed to identify and remove invalid or inactive users and accounts. User Content is continuously backed up, and access controls are implemented to prevent unauthorized modification or access. Regular data integrity checks are performed to ensure the accuracy and completeness of the data. As an additional measure, User Content is versioned and encrypted such that it is possible to revert to a previous state, while verifying integrity. Excessive authentication failures will result in account lockout requiring administrator reset. Redundant systems and data centers are used to ensure high availability, and regular testing and maintenance is performed to prevent system failures. Disaster recovery / business continuity plans are in place to ensure prompt recovery in the event of an emergency situation or disaster. Regular security assessments and penetration testing is performed to identify and address vulnerabilities. Regular training and awareness programs are conducted for personnel to ensure they are aware of security best practices and threats. Regular monitoring and review of the processing systems and services is performed to ensure compliance with this DPA and Applicable Data Protection Laws. Any identified issues are promptly addressed and remediated by the Security Incident Response Team.
Measures for ensuring the ability to restore the availability and access to Personal data in a timely manner in the event of a physical or technical incident	User Content is backed up continuously with verifiable hashes allowing for verification of backup integrity. Multiple geographic zones are in place to ensure service availability is not impacted by a single point of failure. Incident management procedures, as well as business continuity and disaster recovery plans, are in place. User Content is versioned and encrypted such that it is possible to revert to a previous state, while verifying integrity.

Type of measure	Description of measure
Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the Processing	Technical: Product Security, Enterprise Security and Infrastructure security reviews are performed on a continuous basis. Penetration testing is conducted by a third-party on a yearly basis to ensure the robustness of the organization's security controls. Organizational: Yearly disaster recovery and business continuity testing is performed to assess the resilience of our systems. Security awareness training is conducted yearly for all employees, and Secure Development & Data Handling training is provided to employees with access to User Content. All employees must complete an assessment following completion of the training.
Measures for user identification and authorization	Access to the platform is restricted by authentication and authorization policies, implemented within our software stack. Identification is performed by verifying the email and domain of the party accessing the platform. After the party is identified authorization checks are performed to determine the level of access and workspaces which the party has access to. Workspace administrators (customers) are able to authorize additional parties as they see fit.
Measures for the protection of data during transmission	Before data can be transmitted, authentication and authorization take place in order to verify data access rights. Following authorization, a per customer decryption key is used to retrieve the required data, and it is transmitted over a TLS 1.3 encrypted channel.
Measures for the protection of data during storage	All User Content is stored at rest and subject to strict access control. Access to areas housing User Content are limited to services necessary to process the data and to employees with the need to know. Detailed Logging and Monitoring is applied to User Content stores, and alerting is in place to immediately notify the Security Incident Response team of anomalous access. User Content at rest is encrypted with per customer AES-256 keys. These keys are only handled by machine-based services, and not made available to any employees.
Measures for ensuring physical security of locations at which personal data are processed	All xAI facilities are subject to strong physical access requirements. These include restricted entry, controlled ingress, identification of personnel, video surveillance of common areas, and 24/7 physical security monitoring.
Measures for ensuring events logging	User Content access is monitored at multiple points throughout its lifecycle, and centralized in a Security Information and Event Monitoring system. Storage buckets containing data are monitored continuously in real-time through immutable monitoring controls.

Type of measure	Description of measure
Measures for ensuring system configuration, including default configuration	Immutable design principles are in place to ensure that all systems are built in an approved, change-controlled manner. System configuration is applied and maintained by software tools that ensure the system configurations do not deviate from the specifications. A Change Management Policy has been implemented. After systems are deployed, access is restricted such that the integrity of the system infrastructure is not negatively implemented. If any integrity or security issues are discovered the system can safely be rolled back to a previous state.
Measures for internal IT and IT security governance and management and Measures for certification/assurance of processes and products	xAI has in place a written information security policy, including supporting documentation. xAI has a team dedicated to information security, led by the Head of Security. xAI has adopted the NIST 800-171 Rev.3 framework as a baseline for our internal security standards.
Measures for ensuring data minimization	Only the information necessary to provide services is collected during your use of xAI systems, and all User Content is accessed in a de-identified manner. Additionally, data masking is utilized across all systems to ensure User Content is not accessed using sensitive identifiers.
Measures for ensuring data quality	Conducting stress tests of the Grok production system that is equivalent to ten (10) times the expected user base. The purpose of the test is to simulate concurrent access to Grok in order to improve site stability and confirm that the current production system can support the intended target user base.
Measures for ensuring limited data retention	Our data retention period is at our customer's discretion as it regards their user data, subject to legal requirements. Customers are able to delete their data at will. Following a data deletion request, our systems automatically delete all login data, prompt/response pairs, and billing information stored within our systems typically within 30 days.
Measures for ensuring accountability	xAI has established enterprise support and Information Security functions, with established direct lines of contact. xAI's security team is reachable via email at security@x.ai or support@x.ai

EXHIBIT #1
xAI Acceptable Use Policy

xAI Acceptable Use Policy

Effective: January 2, 2025

xAI's Acceptable Use Policy ("AUP") applies to anyone using our Service, including consumers, developers and businesses. We aim to maximize your control over how you use our Service while also ensuring that you do so in a way that is compliant with the law, responsible and safe for humanity. Our policies will evolve over time as our Service and user base change, as well as based on what we learn over time.

By executing a written order for and using our Service, you agree to comply with our policies. Violating our policies could result in action against your account, up to temporary suspension or termination in accordance with the contract Disputes Clause (Contract Disputes Act). Capitalized terms used and not defined herein are defined in the Terms of Service – Enterprise.

You are free to use our Service as you see fit so long as you use it to be a good human, act safely and responsibly, comply with the law, do not harm people, and respect our guardrails:

1. Comply with the law. For example, don't use our Service or Outputs to promote or engage in illegal activities, including:
    1. Violating copyright, trademark, or other intellectual property law
    2. Violating a person's privacy or their right to publicity
    3. Depicting likenesses of persons in a pornographic manner
    4. The sexualization or exploitation of children
    5. Operating in a regulated industry or region without complying with those regulations
    6. Defrauding, defaming, scamming, or spamming
    7. Espionage, spying, stalking, hacking, doxing, or phishing
2. Do not harm people or property. This prohibition includes things like using our Service or Outputs to:
    1. Critically harm or promoting critically harming human life (yours or anyone else's)
    2. Take unauthorized actions on behalf of others
    3. Develop bioweapons, chemical weapons, or weapons of mass destruction
    4. Destroy property
3. Respect guardrails and don't mislead. Don't circumvent safeguards unless you are part of an official Red Team or otherwise have our official blessing. Don't mislead people as to the nature and source of Outputs, including images. You should be transparent and disclose your use of AI assistance and potential limitations, as applicable.

EXHIBIT #2

xAI PRIVACY POLICY

Effective: April 24, 2025

At X.AI LLC ("**xAI**", "**our**", "**us**" or "**we**"), we value your privacy and are committed to being fair, accountable, and transparent in how we handle your personal information. Our Privacy Policy outlines how we collect, use, and disclose your personal information when you use our websites and applications (the Grok mobile app (iOS or Android) or the Grok.com website), and other xAI services (our "**Service**"). It also describes your privacy rights.

This Privacy Policy does not apply to data that we process on behalf of customers of our business offerings, such as the xAI API, or to any employment-related personal information processed in consideration of employment with xAI. This Privacy Policy also does not apply if you access our Service through a third-party's service. In that case, the third-party's privacy policy would apply. For example, your use of X (previously Twitter), including use of Grok on the X platform, is governed by the X Privacy Policy and X Terms, not this xAI Privacy Policy.

For individuals in the European Economic Area, United Kingdom, and Switzerland (collectively, "Europe"), for Europe-specific additional information not already discussed on this page, please see xAI's Europe Privacy Policy Addendum.

1. About xAI and Grok

xAI is a US-based company working on building artificial intelligence tools to accelerate human scientific discovery. We are guided by our mission to advance our collective understanding of the universe. As part of our mission, we have developed "Grok," a conversational generative AI powered by xAI's large language models. More information about xAI's development and training of Grok and data controls is available in our Consumer FAQs, Enterprise FAQs, and xAI website. Please note that xAI is a separate company from X Corp. ("X", previously Twitter).

2. Personal information we collect (Notice at collection)

We ask that you do NOT include personal information in your prompts and inputs into our Service; however, we cannot control what you provide to us.

We may collect personal information from you and about you. Some examples of the information we may collect, how we may collect it, how we may use it, and how we may disclose it are described below.

- **Account Data:** If you create an account with us, we collect your name, contact information, account credentials, and date of birth. Also, to access certain features of the Service, we will collect your date of birth before you may proceed. If you log into our Service using a third-party service, such as X, Google, or Apple, that third-party will send your information to us at your direction. For example, if you use your existing X credentials to log into an xAI mobile app or website, you may choose to direct X to share the following information with us: your X public profile (including profile image), X username, numeric X ID, your date of birth, whether you are subscribed to X Premium, and your Grok on X conversation history.
    - How we may collect it: Directly from you or from a third-party (ex., X, Google, or Apple).
    - How we may use it: To provide, analyze, and maintain our Service; to provide support and assistance in relation to our Service; to develop and improve our Service and to

conduct research; to communicate with you; to ensure the security and integrity of our Service; for legal purposes.
    - How we may disclose it: To our contracted service providers; in connection with business transfers, for legal purposes; to our related companies; and to third-parties with which you interact or share information.

- **Payment Data:** Where payment is required to access the Service (ex., if you are paying for a subscription), we may have a third-party process payment information, such as payment card information, and details regarding your transactions for us.
    - How we may collect it: Through a third-party processor (ex., Apple App Store, Google Play Store, or Stripe).
    - How we may use it: To provide, analyze, and maintain our Service; to provide support and assistance in relation to our Service; to ensure the security and integrity of our Service; for legal purposes.
    - How we may disclose it: To our contracted service providers; in connection with business transfers, and for legal purposes.

- **Communication Data:** If you communicate with us, such as by email, by our webpages, or on social media sites, we may collect personal information that you submit to us including your name, user name, email address, any other information you voluntarily choose to provide us, and the contents of messages you send.
    - How we may collect it: Directly from you.
    - How we may use it: To provide, analyze, and maintain our Service; to provide support and assistance in relation to our Service; to develop and improve our Service and to conduct research; to communicate with you; to ensure the security and integrity of our Service; for legal purposes.
    - How we may disclose it: To our contracted service providers; in connection with business transfers, for legal purposes; and to our related companies.

- **User Content:** You may provide personal information in prompts and other content you input, such as files, images, audio, voice, video, and other material (“Input”). Outputs of the Service (“Output”), including responses Grok generates, are based on your Input (together, "User Content"). If you include personal information in Inputs you provide to the Service, this information may be reproduced in the Output.
    - How we may collect it: Directly from you.
    - How we may use it: To provide, analyze, and maintain our Service; to provide support and assistance in relation to our Service; to develop and improve our Service and to conduct research; to ensure the security and integrity of our Service; for legal purposes.
    - How we may disclose it: To our contracted service providers; in connection with business transfers, for legal purposes; and to our related companies.

- **Feedback Data:** Where applicable, we will collect your Feedback (as defined in our Terms of Service). This might arise if, for example, in a given conversation with Grok, you rate an Output using the thumbs-up/thumbs-down icons.
    - How we may collect it: Directly from you.
    - How we may use it: To provide, analyze, and maintain our Service; to provide support and assistance in relation to our Service; to develop and improve our Service and to conduct research; to ensure the security and integrity of our Service; for legal purposes.

    - How we may disclose it: To our contracted service providers; in connection with business transfers, for legal purposes; and to our related companies.

- **Social Media Information:** We have pages on social media sites like Instagram, Facebook, Medium, X, YouTube, and LinkedIn. When you interact with our social media pages, we collect personal information that you choose to provide to us. In addition, the companies that host our social media pages may provide us with aggregate information and analytics about our social media activity.
    - How we may collect it: Directly from you or from companies that host our social media pages.
    - How we may use it: To provide, analyze, and maintain our Service; to provide support and assistance in relation to our Service; to develop and improve our Service and to conduct research; to communicate with you; to ensure the security and integrity of our Service; for legal purposes.
    - How we may disclose it: To our contracted service providers; in connection with business transfers, for legal purposes; to our related companies; and to third-parties with which you interact or share information.

- **Technical Data:** Technical data includes information such as your IP address, device type, country from which you access, analytics information, browser type and version, browser plug-in types and versions, and operating system. This may also include information about your use of the Service and how you interact with the Service, including the types of content you view or engage with, the features you use, pages you view and your Grok conversation history.
    - How we may collect it: Automatically when you use or interact with the Service, including through analytics tools.
    - How we may use it: To provide, analyze, and maintain our Service; to provide support and assistance in relation to our Service; to develop and improve our Service and to conduct research; to communicate with you; to ensure the security and integrity of our Service; for legal purposes.
    - How we may disclose it: To our contracted service providers; in connection with business transfers, for legal purposes; and to our related companies.

- **Location data:** We may determine the general area from which your device accesses our Services based on information like its IP address. Also, you may choose to provide more precise location information, such as your address, your device's GPS location, or location information from third-party services that you use. We obtain your consent prior to collecting precise location information.
    - How we may collect it: Directly from you or from third-party services that you use.
    - How we may use it: To provide, analyze, and maintain our Service; to provide support and assistance in relation to our Service; to develop and improve our Service and to conduct research; to communicate with you; to ensure the security and integrity of our Service; for legal purposes.
    - How we may disclose it: To our contracted service providers; in connection with business transfers, for legal purposes; to our related companies; and to third-parties with which you interact or share information.

- **Publicly Available Data:** We use information that is publicly available on the internet to train our models and provide resulting Output. While we do not intentionally seek out personal information,

we understand that there is personal information incidentally included in these datasets. For more information on the sources of information used in the development and operation of our large language models, see our Consumer FAQs.
    - How we may collect it: From publicly available resources and providers.
    - How we may use it: To provide, analyze, and maintain our Service; to develop and improve our Service and to conduct research; to ensure the security and integrity of our Service; for legal purposes.
    - How we may disclose it: To our contracted service providers; in connection with business transfers, for legal purposes; and to our related companies.

- **Public X Posts and Internet Search Data:** The Service uses public posts shared on X, engagement data such as number of followers, and number of views, likes, reposts, shares, and replies and internet search results. In some instances, this data may include personal information.
    - How we may collect it: Public X posts are provided by X and internet search data is provided by internet search providers.
    - How we may use it: To provide, analyze, and maintain our Service; to provide support and assistance in relation to our Service; to develop and improve our Service and to conduct research; to ensure the security and integrity of our Service; for legal purposes.
    - How we may disclose it: To our contracted service providers; in connection with business transfers, for legal purposes; and to our related companies

We do not aim to collect sensitive personal information (ex., information related to racial or ethnic origin, political opinions, religion or other beliefs, health, biometric scans, criminal background, or trade union membership) and ask that you do not provide us with any such information. In addition, in relation to Grok's training, xAI does not process training data for the purposes of inferring or deriving any sensitive or special category data about individuals, and we do not actively seek out data sources that include sensitive or special category data.

3. How we may use personal information

We may use your personal information for a variety of purposes. Below, you will find examples and additional information regarding how we may use your personal information.

- To provide, analyze, and maintain our Service: For example, to respond to your Inputs (including when you type text prompts or when you give spoken prompts) to Grok or to process payments for subscriptions to our Service.
- To provide support and assistance in relation to our Service: For example, to troubleshoot problems and to provide customer support.
- To develop and improve our Service and to conduct research: For example to develop new product features, to train our models, to identify usage trends, to operate and expand our business activities, to identify new customers, and for data analysis.
- To communicate with you: For example, to send you information about our Service, events, or changes to the Service. This may include sending you non-promotional emails, such as emails about your Grok access, legally required notices, or our ongoing business relations.
- To ensure the security and integrity of our Service: For example, to protect the security of our Services and to detect and prevent fraud, unauthorized use, unlawful activity, and other misuses of our Service.
- For legal purposes: For example, to comply with our legal obligations and to protect the rights, privacy, safety, or property of our users, xAI, or third-parties. This may include detecting what country you are located in so we can comply with relevant legal obligations.

We may aggregate, pseudoanonymize, or de-identify your information so that it no longer identifies you and use this information for the purposes described above, such as to analyze the way our Service is being used, to improve and add features to them, and to conduct research. We will maintain and use pseudoanonymized or de-identified information in pseudoanonymized or de-identified form and will not attempt to reidentify the information, unless required by law.

We do not sell your personal information or use it for marketing: We do not sell personal information or share personal information for targeted or cross-contextual advertising purposes. We do not collect and use your personal information for marketing purposes and do not share your personal information with third-parties for the purpose of marketing.

4. How we may disclose personal information

We may disclose your personal information to others. Below, you will find examples and additional information regarding how we may disclose your personal information.

- To our contracted service providers: To assist in providing the Service to you or performing business operations, we provide your personal information to service providers including providers of hosting, cloud, analytics, content delivery, support and safety monitoring, payment and transaction, and other technology services, for the purposes described above.
- In connection with business transfers: In connection with or during negotiation of any merger, financing, acquisition, bankruptcy, dissolution, transaction, or proceeding involving sale, transfer, divestiture, or disclosure of all or a portion of our business or assets to another company. If required by applicable laws, we will use reasonable efforts to notify you of any transfer of personal information to an unaffiliated third-party.
- For legal purposes: To (i) comply with laws or to respond to lawful requests and legal process, (ii) protect the rights and property of xAI and our agents, customers, and others, including to enforce our agreements, policies, and terms of service, (iii) to protect against legal liability, or (iv) to protect the personal safety of xAI, its customers, or any person.
- To our related companies: To our related companies to the extent such sharing is necessary to fulfill a request you have submitted via our Service or for customer management, customer support, technical operations, or the purposes described above.
- To third-parties with which you interact or share information: Certain features may allow you to share information with third-parties, such as through the X platform. Information you share with third-parties is governed by that third-party's terms and policies.

5. Retention of personal information

We retain your personal information where we have an ongoing legitimate business need to do so. In certain circumstances, we will retain your information for legal reasons after our contractual relationship has ended. The specific retention periods depend on the nature of the information and why it is collected and processed and the nature of the legal requirement. For example, we may retain your personal information:

- When we have a legal obligation to do so (e.g., if we receive a court order, we would retain your information for longer than our usual retention periods);
- To address and resolve requests and complaints (e.g., if there is an ongoing complaint about you);
- To protect the safety, security, and integrity of our business and the Service, as well as to protect our rights and property and those of others (e.g., if we detect misuse of our Service or otherwise detect unusual activity on your account or in your interactions with us); and
- For litigation, regulatory or other legal matters (e.g., we would retain your information if there was an ongoing legal claim and the information was relevant to the claim).

The length of time we retain data may depend on the features or settings you use. For example, when Private Chat is turned on, conversations will not appear in your conversation history and your conversations will be deleted from xAI systems within 30 days unless it is necessary that they be kept longer for legal, compliance, or safety purposes. Further, if you choose to delete any or all of your conversations or if you choose to delete your account, we will delete the data within 30 days unless it is necessary to retain the data for legal, compliance, or safety purposes.

6. Security of personal information

xAI implements commercially reasonable technical, administrative, and organizational measures designed to protect personal information from loss, misuse, and unauthorized access, disclosure, alteration, or destruction. However, no security measure or method of data transmission over the internet is 100% secure. In addition, you are solely responsible for protecting your log-in and password, limiting access to your devices, and signing out of websites and accounts after your sessions.

7. Links to other websites

Our Service may contain links to external websites or social media platforms that are not operated by us. Third-party websites and services have their own terms and conditions and privacy policies, and you should read these carefully before you submit any personal information to them.

8. Children under the age of 13

As noted in the Terms of Service, our Service is not directed at children or minors under the age of 13 and we do not knowingly collect any personal information from them. While we have taken measures to limit undesirable training data and outputs, Grok could produce output that is not appropriate for all ages. Parents of teenagers between the ages of 13 and 17 years old must agree to the Terms of Service and are urged to exercise care in monitoring the use of this Service by their teenagers. Depending on how a user interacts with the Service, including which modes the user purposely selects, the Service may have content such as some suggestive dialogue, coarse language, crude humor, sexual situations, or violence. If you are a child under the age of 13, please do not attempt to register for or otherwise use our Service. Please contact us here if you are aware that we may have inadvertently collected personal information from a child under the age of 13.

9. Privacy rights and choices

Depending on where you are located and subject to applicable legal exceptions, you may have certain rights in relation to your personal information. For information on the privacy rights that may be available to you under European privacy laws, please review xAI's Europe Privacy Policy Addendum.

- You may have the right to request to access, correct, update or delete your personal information, subject to certain applicable legal exceptions.
  Please note that we cannot guarantee the factual accuracy of Output from our models. If Output contains factually inaccurate personal information relating to you, you can submit a correction request and we will make reasonable efforts to correct this information — but due to the technical complexity of our models, it may not be feasible for us to do so.
- If we have collected and processed your personal information with your consent, then you can withdraw your consent at any time. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal information conducted in reliance on lawful processing grounds other than consent.
- The right to submit certain privacy requests through an Authorized Agent.
- The right to be free from discrimination for exercising the rights afforded to you under applicable privacy laws.
- The right to appeal a decision we make about your rights request.

Exercising your rights: Some of these rights may be exercised in the xAI Service but for others you will need to submit a request at https://xai-privacy.relyance.ai/ and include your full legal name, email address, and city, state/province, and country of residence. Once you have submitted your request, we will respond within the time frame permitted by applicable privacy laws.

Please note, however, that your personal information may be exempt from such requests in certain circumstances, for example if we need to keep using your information to comply with our own legal obligations or to establish, exercise or defend legal claims. If an exception applies, we will inform you when responding to your request.

Verification: In order to protect your personal information, your ability to exercise some of the rights detailed in this Privacy Policy may be subject to your ability to verify that you are the person about whom your request pertains. For example, we may require you to verify your identity by validating your account credentials or submitting additional information to allow us to verify your identity.

Authorized Agents: To exercise your rights using an Authorized Agent (as defined under applicable law), you must provide your Authorized Agent with written permission to exercise your rights on your behalf, and we may request a copy of this written permission from your Authorized Agent when they make a request on your behalf. We reserve the right to deny a request from an Authorized Agent that does not submit proof that they have been authorized by you to act on your behalf.

Appeals: If we refuse to take action on a request within a reasonable period of time after receiving your request, you may appeal our decision via https://xai-privacy.relyance.ai/. In such an appeal, you must (1) provide sufficient information to allow us to verify that you are the person about whom the original request pertains and to identify the original request, and (2) provide a description of the basis of your appeal. Please note that your appeal will be subject to your rights and obligations afforded to you under applicable law. We respond to all appeal requests as soon as we reasonably can, and no later than legally required.

For more information on your rights with respect to data we use to train our models, please read our Consumer FAQs.

Do Not Track: Please note that because the effect of "Do Not Track" signals remains unclear, and because there continues to be no consistent industry understanding of how to respond to such a signal, we do not alter our privacy practices when we detect a "Do Not Track" signal from your browser.

10. Changes to this Privacy Policy

We may update our Privacy Policy from time to time. When we do, we will publish an updated version and effective date on this page, unless another type of notice is required by applicable law. If you use the Service after any changes to the Privacy Policy have been posted, all of the changes made will apply to your use of the Service.

11. Child safety issues

To report child safety issues to us, please contact us here.

Residents of Australia can find resources regarding child safety and reporting here.

12. How to contact us about privacy requests

If you have any queries or complaints about our collection, use, or storage of your personal information, or if you wish to exercise any of your rights in relation to your personal information, please contact us at https://xai-privacy.relyance.ai/ or by the following contact details:

- For the fastest response for world-wide requests and in the USA: x.AI LLC, https://xai-privacy.relyance.ai/

- Other contacts for privacy requests:
- In the UK: Lionheart Squared Limited, FAO x.ai, 17 Glasshouse Studios, Fryern Court Road, Fordingbridge, Hampshire, SP6 1QX United Kingdom xai@lionheartsquared.co.uk
- In the EU: Lionheart Squared (Europe) Ltd, FAO x.ai, 2 Pembroke House, Upper Pembroke Street 28-32, Dublin, D02 EK84, Republic of Ireland xai@lionheartsquared.eu
- In Switzerland: Lionheart Squared Switzerland SarL, FAO x.ai, Blvd George Favon 43, CH-1204 Geneva, Switzerland xai@lionheartsquared.ch
- You can contact our Data Protection Officer: Taceo Limited, Riverbank House, 2 Swan Lane, London EC4R 3T dpo@taceo.co.uk