xAI Privacy Notice
to Employees, Contractors, and Job Candidates

Last Updated: March 17, 2025

X.AI LLC. (together with its subsidiaries and affiliates, the "**Company**," **"xAI,"** "**us**" or "**we**") is committed to protecting the privacy of the personal information of our current and former employees (collectively, "**Employees**") and job applicants and contractors (collectively, "**Personnel**" or "**you**") and their emergency contacts and beneficiaries.

This Global Employee Privacy Notice ("**Notice**") applies to the Company's collection and use of the personal information in compliance with applicable data protection and privacy laws, including but not limited to the California Consumer Privacy Act (CCPA), the EU General Data Protection Regulation (GDPR) (including Article 9), UK GDPR, the Swiss Federal Act on Data Protection (FADP), Argentina's Personal Data Protection Law (PDPL), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), and Australia's Privacy Act.

Please read this Notice carefully because it provides important information and explains your rights. If you have any questions or concerns, or wish to exercise your privacy rights, we invite you to contact us by any of the methods listed at the bottom of this Notice.

As we continually work to improve our operations and business, we may update this Notice from time to time and will notify when we do.

Personal Information We Collect

This chart details the categories of personal information that we collect (Notice at Collection) and have collected over the past twelve (12) months:

Category of Information	Examples of Personal Information We Collect	Categories of Third Parties With Whom We Share This Personal Information
Identifiers	● Real name ● Alias ● Postal address ● Unique personal identifier (including, telephone number or device identifier) or online identifier ● Email address	● Service Providers ● Affiliates

Category of Information	Examples of Personal Information We Collect	Categories of Third Parties With Whom We Share This Personal Information
	● Account name ● Social security number ● Driver's license number or passport number ● Other similar identifiers	
Categories of Personal Information Described in California Customer Records Act (Cal. Civ. Code § 1798.80(e))	● Name ● Signature ● Social security number ● Physical characteristics or description ● Address ● Telephone number ● Passport number, driver's license or state identification card number ● Insurance policy number ● Educational information ● Employment or employment history ● Bank account number, credit card number, debit card number or any other financial information ● Medical information or health insurance information. We process this special category of data only where permitted by applicable law and with appropriate safeguards, including: (i) with your explicit consent; (ii) to carry out our obligations in the field of employment law, social security and social protection; (iii) to protect your vital interests where you are physically or legally incapable of giving consent; (iv) for the establishment, exercise or defense of legal claims; or (v) for occupational medicine, assessment	● Service Providers ● Affiliates

Category of Information	Examples of Personal Information We Collect	Categories of Third Parties With Whom We Share This Personal Information
	of working capacity, or provision of health or social care.	
Characteristics of Protected Classifications	● National origin ● Physical or mental disability (which will only be processed where explicitly permitted by applicable data protection laws, including GDPR Article 9 and similar provisions in other jurisdictions, with appropriate safeguards in place) ● Medical condition (which we process only where permitted by applicable law, such as with explicit consent, to comply with employment law obligations, or to protect vital interests, and with appropriate safeguards in accordance with GDPR Article 9 and similar provisions in other applicable jurisdictions) ● Marital status ● Sex, gender, gender identity, or gender expression ● Age ● Military and veteran status	● Service Providers ● Affiliates
Commercial Information	● Records of personal property, products or services purchased, obtained or considered ● Other purchasing or consuming histories or tendencies	● Service Providers ● Affiliates
Biometric Information	● Fingerprints (used to access devices such as company computers)	Not shared
Internet or Other Electronic Network Activity Information	● Browsing history or search history ● Information regarding Personnel's interaction with an internet website, application, or	● Service Providers ● Affiliates

Category of Information	Examples of Personal Information We Collect	Categories of Third Parties With Whom We Share This Personal Information
	advertisement (including chats and instant messaging)	
Geolocation Data	● IP-address-based location information	● Service Providers
Photos, Videos, or Recordings	● Photos, videos or recordings of Personnel ● Photos, videos or recordings of Personnel environment	● Service Providers ● Affiliates
Security Monitoring (including for investigations, compliance, and legal matters)	● System logs ● Security event data ● Access logs and access patterns ● Network traffic ● Communications (including emails, messaging, and texts) using Company systems, applications, or devices ● Key logging ● Screen recordings	● Service Providers ● Affiliates
Social Media Monitoring	● Public posts mentioning the Company ● Professional social media profiles ● Work communications on company platforms	● Affiliates ● Service Providers
Internet Monitoring	● Browsing history ● Time spent online ● Bandwidth usage	● Affiliates ● Service Providers
Professional or Employment-Related Data	● Resume ● Job title ● Job history ● Performance evaluations ● Union membership ● Performance management information, such as employment status (full-time or part-time, regular or temporary), work schedule, job assignments, hours worked, accomplishments and awards ● Training and development information ● Discipline and counselling information	● Service Providers ● Affiliates

Category of Information	Examples of Personal Information We Collect	Categories of Third Parties With Whom We Share This Personal Information
	● Employment termination information	
Education Information (including as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99))	● Grades or transcripts ● Student disciplinary records	● Service Providers ● Affiliates
Categories of Personal Information Considered "Sensitive" Under the California Privacy Rights Act	● Social security, driver's license, state identification card or passport numbers ● Account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password or credentials allowing access to an account	● Service Providers ● Affiliates
Inferences Drawn From Other Personal Information Collected	● N/A	
Other	● Personal information about Employees' dependents under the age of 16. ● Emergency contact information (including, name, postal address, telephone number and relationship to Employee) ● Beneficiary information (including, name, postal address, telephone number, birth date, social security number and relationship to Employee)	● Service Providers

- **Purpose of Collection**: The personal information collected is used to operate, manage, and improve our operations and business, to perform our contract with you, to provide services and benefits to our employees and contractors, and to comply with legal obligations.

- **Use of Personal Information**: We use personal information for the purposes described in this Privacy Notice, including but not limited to employment and business operation purposes, legal compliance, and security. In some cases, we or third parties may have legitimate interests in using your personal information.

- **Sharing of Personal Information**: We may share your personal information with our affiliates, service providers, and other third parties as outlined in this Privacy Notice.

- **Your Privacy Rights**: You have certain rights with respect to your personal information, as detailed in this Privacy Notice, including the right to access, correct, and delete your personal information.

- **Contact Information**: For any questions or to exercise your rights, please contact us at https://privacy.x.ai/.

By providing your personal information, you acknowledge that you have read and understood this notice and consent to the collection, use, and sharing of your personal information as described herein and in our Privacy Notice.

Sources of Personal Information

We may collect personal information from the following categories of sources, as permitted by applicable law and where relevant to the purposes described in this Privacy Notice:

- You
    - When you provide such information directly to us.
- Public Records
    - From publicly available government records and other public sources, where permitted by applicable law.
- Third Parties, where they have the right to share such information with us and in accordance with applicable privacy laws. Such third parties may include:
    - Vendors
        - Recruiters.
        - Pre-employment screening services.
        - Credentialing and licensing organizations.
        - Consumer reporting agencies and credit information. The Company complies with applicable consumer reporting and credit information laws, including but not limited to the Fair Credit Reporting Act (FCRA) in the United States, the Consumer Reporting Act in Canada, and similar applicable laws in other jurisdictions. Before obtaining any consumer reports or credit information, the Company will obtain all necessary consents and provide required disclosures to the relevant

individuals in accordance with applicable law. Where required by law, individuals will be notified of any adverse actions taken based on information obtained from consumer reporting agencies. The Company monitors public social media activity related to the Company based on legitimate interests

- o Prior employers (e.g., for references)
- o Professional references
- o Educational institutions
- o Publicly Available Sources
  - Examples publicly available professional profiles and information on platforms like LinkedIn, Twitter and Facebook.

Our Commercial or Business Purposes for Collecting or Disclosing Personal Information of Employees

- Employing and/or Engaging Personnel and Operating, Hosting and Facilitating Our Operations and Business
  - **o** Processing and managing Personnel applications.
  - **o** Conducting background and reference checks.
  - **o** Providing immigration support.
  - **o** Entering into contracts.
  - **o** Onboarding Personnel.
  - o Enrolling and administering employment benefits.
  - o Paying Personnel.
  - o Implementing, managing and improving the Company's recruitment process.
  - o Implementing health and safety measures and maintaining a safe workplace, assessing Personnel working capacity and administering health and Workers' Compensation insurance programs. Where this involves processing health data or other special categories of personal data, we do so in accordance with applicable data protection laws, including Article 9 of the GDPR, and only where we have a valid legal basis such as: explicit consent, compliance with employment law obligations, assessment of working capacity, or other permitted grounds under applicable law. We implement appropriate technical and organizational measures to protect such sensitive data.
  - o Ensuring that Personnel properly log in to Company equipment, systems and applications, and ensuring that authorized Personnel have access to secured locations in the Company, including monitoring and logging such access for security purposes in accordance with applicable laws and internal policies.
  - o Managing workflow, dispatching Personnel to customers, and performing services for the Company's customers.

- Managing the Company's relationship with Personnel.
- Carrying out job promotion processes, including to evaluate Employees for promotions.
- Featuring Employees in marketing materials and on the Company's website.
- Meeting or fulfilling the reason you provided the information to us.
- Maintaining the security of our systems and property, including: (i) monitoring and logging of Company system, application, and device access and usage; (ii) conducting regular security audits and vulnerability assessments; (iii) implementing and maintaining incident response procedures; (iv) performing fraud and trade secret disclosure detection and prevention activities; and (v) carrying out security-related debugging and system maintenance.
- Carrying out other business or employment-related purposes stated when collecting your personal information or as otherwise set forth in applicable data privacy laws, including but not limited to the CCPA, GDPR, UK GDPR, and other applicable privacy laws.

- Meeting Legal Requirements and Enforcing Legal Terms
  - Fulfilling our legal obligations under applicable law, regulation, court order or other legal process, such as preventing, detecting and investigating security incidents and potentially tortious, illegal, or prohibited activities, or responding to lawful requests by public authorities, including to meet national security or law enforcement requirements, subject to appropriate legal safeguards and in accordance with applicable data protection laws.
  - Protecting the rights, property or safety of you, the Company or another party.
  - Enforcing any agreements with you.
  - Responding to claims.
  - Resolving disputes.

- Technology Resource Monitoring
  The Company monitors and processes information from technology resources in accordance with applicable data protection laws. This processing is based on legitimate business interests, legal obligations, contractual necessity or your consent where required.
  - Protecting company systems and data, ensuring network and information security
  - Protecting Company's confidential information
  - Preventing and detecting criminal activity
  - Ensuring compliance with security policies
  - Detecting and preventing security incidents
  - Meeting regulatory obligations
  - Ensuring compliance with company policies

- The Company will monitor Company system, application, and device activities to detect, prevent, and respond to potential security threats, unauthorized access, malicious or illegal activities, or policy violations to maintain the integrity and confidentiality of the system. Any monitoring will be proportionate, transparent, and respect employees' privacy rights in accordance with applicable laws
    - Monitoring of system resources will be conducted to ensure optimal allocation and utilization of computing resources, storage capacity, and network bandwidth, enabling efficient system performance and cost management.
    - The Company shall monitor activities to ensure compliance with internal policies, regulatory requirements, and industry standards, maintaining documentation and audit trails as required by applicable laws.
    - Regular monitoring of system performance metrics will be implemented to identify bottlenecks, optimize system efficiency, and ensure service level agreements are met, enabling proactive maintenance and continuous improvement of system operations.
    - The Company shall monitor the internet usage for the following reasons:
        - EU/UK GDPR: Article 6(1)(f) legitimate interests
        - CCPA: Business purpose - security and compliance
        - PIPEDA: Reasonable purpose for network management
        - FADP: Justified business interest
        - LatAm: Employment relationship basis

We will not collect additional categories of personal information or use the personal information we collected for materially different, unrelated or incompatible purposes without providing you prior notice and, where required by applicable law, obtaining your consent.

How We Share Personal Information

We disclose your personal information to the categories of service providers and other parties listed in this section.

- Affiliates. Our affiliates help us to perform business functions on our behalf.
- Service Providers. These parties help us to perform business functions on our behalf. They include:
    - Hosting, technology and communication providers.
    - Security and fraud prevention consultants.
    - Background and reference check screening services.
    - Hiring process and benefits management and administration tools.

We may share personal information as described in this Privacy Notice in accordance with applicable data protection and privacy laws, including but not limited to the EU/UK GDPR, Swiss FADP, CCPA, PIPEDA, Australian Privacy Principles, Argentine PDPL, and Colombian Law 1581 of 2012.

- Personal information may be shared with the following categories of recipients when necessary and proportionate to achieve specified purposes:
    - Law enforcement authorities, courts, and government officials when legally required or authorized by applicable law
    - Regulators and supervisory authorities
    - Legal advisors and professional consultants
    - Service providers and business partners
    - Other third parties as required by law or to protect rights

- Our sharing of personal information is based on specific legal grounds and legitimate purposes, as required by applicable privacy laws, including:
    - Compliance with legal obligations under applicable laws and regulations
    - Exercise, establishment, or defense of legal rights and claims
    - Protection of vital interests of data subjects or other persons
    - Legitimate business interests, where not overridden by individual rights
    - Performance of contractual obligations, where applicable

- When transferring personal information across borders, we implement safeguards to ensure adequate protection of your data. These international transfers are conducted only when necessary and with appropriate security measures in place, including:
    - Standard Contractual Clauses approved by relevant authorities
    - Intra-Group Data Processing Agreement, where applicable
    - Adequacy decisions issued by competent authorities
    - Other valid transfer mechanisms as required by applicable laws

- This sharing is conducted in compliance with:
    - EU/UK GDPR (Articles 6, 13, 14, 44-50)
    - California Privacy Rights Act (CPRA/CCPA)
    - Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)
    - Australian Privacy Principles (APP)
    - Swiss Federal Act on Data Protection (FADP)
    - Argentine Personal Data Protection Law (PDPL)
    - Colombian Law 1581 of 2012

We employ data minimization and necessity practices. In addition, we maintain required records in accordance with applicable laws.

Business Transfers

Your personal information that we collect may be transferred to a third party if we undergo a merger, acquisition, bankruptcy or other transaction in which that third party assumes control of our business (in whole or in part). Should one of these events occur, we will notify you, if applicable law requires.

Information that is Not Personal Information

We may create aggregated, de-identified or pseudo-anonymized data from the personal information we collect, including by removing information that makes the data personally identifiable to a particular member of our Personnel. We may use such aggregated, de-identified or pseudo-anonymized data and share it with third parties for our lawful business purposes, including to operate, host and facilitate our operations and business, provided that we will not share such data in a manner that could identify you.

Data Security

We seek to protect your personal information from unauthorized access, use and disclosure using appropriate physical, technical, organizational and administrative security measures based on the type of personal information and how we are processing that information. Our data protection measures include industry-standard data protection techniques, including de-identification, data masking, pseudonymization, access level controls, and encryption used in applicable scenarios. We also have periodic security assessments. You should also help protect your data by appropriately selecting and protecting your password and/or other sign-on mechanism, limiting access to your computer or device and browser, and signing off after you have finished accessing your account. Although we work to protect the security of your account and other data that we hold in our records, please be aware that no method of transmitting data over the internet or storing data is completely secure.

Data Retention

We retain personal information about you for as long as necessary to perform our business or commercial purposes, including employment-related purposes, and to comply with U.S. Federal and state laws and other applicable laws.

When establishing a retention period for specific categories of personal information, we consider who we collected the personal information from, our need for the personal

information, why we collected the personal information, and the sensitivity of the personal information.

Employment-related data is retained for at least 7 years after the last date of employment to comply with laws and regulations. In some cases, we retain personal information for longer, if doing so is necessary to comply with our legal obligations, resolve disputes or collect fees owed, or is otherwise permitted or required by applicable law, rule or regulation. We may further retain information in an anonymous or aggregated form where that information would not identify you personally.

Your Privacy Rights

You have the rights set forth in this section, which vary depending on your jurisdiction and the applicable privacy laws (including but not limited to EU GDPR, UK GDPR, CCPA, and other applicable privacy regulations). Please see the "Exercising Your Rights" section below for instructions regarding how to exercise these rights in your jurisdiction.

Access

You have the right to request certain information about our collection and use of your personal information for the time period required by applicable law:

- The categories of personal information that we have collected about you.
- The categories of sources from which that personal information was collected.
- The business or commercial purpose for collecting or selling your personal information.
- The categories of third parties with whom we have shared your personal information.
- The specific pieces of personal information that we have collected about you.

For California residents: if we have disclosed your personal information to any third parties for a business purpose over the past twelve (12) months, we will identify the categories of personal information shared with each category of third-party recipient.

For individuals in the European Economic Area (EEA), United Kingdom, and Switzerland, we process your personal data on the following legal bases under the GDPR and UK GDPR: (i) your consent; (ii) performance of a contract with you; (iii) compliance with our legal obligations; (iv) protection of your vital interests; (v) performance of a task carried out in the public interest; and/or (vi) our legitimate interests or those of a third party. For transfers of personal data from these regions to the United States within our group of companies, we rely on our intra-group data transfer agreement. For transfers to third parties outside these regions, we implement appropriate safeguards, including the European Commission's Standard Contractual Clauses (SCCs).

For individuals in Argentina, you have rights under the Personal Data Protection Law No. 25,326, including rights to access, correct, and delete your personal data. For individuals in Australia, you have rights under the Privacy Act 1988, including the right to access and correct your personal information. For individuals in Canada, you have rights under PIPEDA, including the right to access your personal information and challenge its accuracy. For individuals in Colombia, you have rights under Law 1581 of 2012, including rights to access, update, and rectify your personal data.

If we have sold your personal information over the past twelve (12) months, we will identify the categories of personal information sold to each category of third-party recipient.

Deletion

You have the right to request that we delete the personal information that we have collected about you. Under applicable privacy laws, you have the right to request deletion of your personal information. We will respond to deletion requests within the following timeframes:

- EU/UK (GDPR): Without undue delay and within one month (may be extended by two months for complex cases)

- California (CCPA): Within 45 business days (may be extended by 45 additional days when reasonably necessary)

- Switzerland (FADP): Within 30 days

- Canada (PIPEDA): Within 30 days

- Australia (Privacy Act): Within 30 days

- Argentina (Law 25,326): Within 10 working days

- Colombia (Law 1581): Within 15 working days

This right is subject to certain exceptions, such as when we need to retain your personal information to comply with legal obligations or when deletion involves disproportionate effort. These rights apply to employees as permitted by applicable law, with specific provisions for employee data under each jurisdiction's requirements. If your deletion request is subject to any exceptions, we may deny your deletion request.

Correction

In some jurisdictions, you have the right to request that we correct any inaccurate or incomplete personal information we have collected about you. This right (also known as the "right to rectification" or "right to correction" and regulations worldwide. You may

exercise this right free of charge, subject to verification of your identity and the following jurisdiction-specific requirements) is guaranteed under various privacy laws:

(i) Article 16 of the EU GDPR and UK GDPR; (ii) the Swiss Federal Act on Data Protection (FADP); (iii) the California Consumer Privacy Act (CCPA); (iv) the Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada; (v) the Privacy Act 1988 of Australia; (vi) the Personal Data Protection Law of Argentina; and (vii) Colombian Law 1581 of 2012

The timeframe for responding to your correction request varies by jurisdiction. We will process your request without undue delay, and within the following statutory timeframes:

- EU/UK (GDPR): Within one month (may be extended by two months for complex cases)

- California (CCPA): Within 45 business days

- Switzerland (FADP): Within 30 days

- Canada (PIPEDA): Within 30 days (may be extended by 30 days if necessary)

- Australia (Privacy Act): Within 30 days

- Argentina (Law 25,326): Within 10 working days

- Colombia (Law 1581): Within 15 working days

These rights apply to both consumers and employees where permitted by law. Note that employee data rights may vary:

- In California, employee rights under CCPA became effective January 1, 2023

- Under EU/UK GDPR, employees have full data subject rights

- Under PIPEDA, employee rights apply only to federal works, undertakings, and businesses

- In Australia, employee records are exempt from the Privacy Act in certain circumstances

We may deny your correction request if we determine, based on the totality of circumstances, that your personal information is already accurate and complete. If your request is denied under relevant privacy laws, we will provide you with a detailed explanation of our decision.

Right to Data Portability

For individuals within the European Union and the United Kingdom, under Article 20 of the GDPR and UK GDPR, you have the right to receive your personal data, which you have provided to us, in a structured, commonly used, and machine-readable format. You also have the right to transmit this data to another data controller without hindrance from us. This right applies when processing is based on consent or a contract and is carried out by automated means. In the United States, Canada, Australia, Argentina, and Colombia, the right to data portability will be honored in accordance with applicable local privacy laws, where such rights are recognized. Employees in these jurisdictions may request data portability by contacting our privacy team at https://privacy.x.ai/. We will respond to your request within the statutory timeframe applicable to your jurisdiction.

Automated Individual Decision-Making

For individuals in the European Union and the United Kingdom, under Article 22 of the GDPR and UK GDPR, you have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning you or similarly significantly affects you. This right does not apply if the decision is necessary for entering into or performing a contract between you and us, is authorized by law, or is based on your explicit consent. In the United States, Canada, Australia, Argentina, and Colombia, the right to object to automated decision-making will be respected in accordance with local privacy laws, where such rights exist. Employees who wish to exercise this right should contact the privacy team at https://privacy.x.ai/.

Processing of Sensitive Personal Information

We collect personal information that is considered “sensitive personal information” under the CCPA, "special categories of personal data" under the GDPR/UK GDPR (including health data), "sensitive information" under the Australian Privacy Act, "datos sensibles" under Colombian and Argentinian privacy laws, as well as sensitive information under other applicable privacy laws. When processing special categories of personal data under the GDPR/UK GDPR, including health data, we do so where: (1) we have obtained your explicit consent; (2) processing is necessary for carrying out obligations under employment, social security or social protection law; (3) processing is necessary to protect your vital interests where you are physically or legally incapable of giving consent; or (4) processing is necessary for the establishment, exercise or defense of legal claims. For California residents, consumers have specific rights regarding their sensitive personal information. Similar rights exist under other privacy laws, including enhanced protections for sensitive data under the EU GDPR, UK GDPR, Swiss DPA (including specific Swiss requirements for processing "personality profiles" and sensitive personal data under Articles 4 and 6 of the Swiss DPA, which require explicit justification grounds and enhanced protection measures), and other applicable privacy regulations. we only use or disclose your sensitive personal information for limited purposes as required by law, including: providing services you've requested, ensuring security and integrity, short-term transient use, performing services on

behalf of the business, and other purposes permitted under section 7027(m) of the CCPA regulations and we do not collect or process sensitive personal information with the purpose of inferring any characteristics about California residents. Additionally, in accordance with the GDPR, UK GDPR, and other applicable privacy laws, we do not process sensitive personal data for behavioral advertising or profiling purposes without explicit consent, and where such consent is obtained, we provide clear mechanisms for withdrawing consent at any time, in accordance with the consent withdrawal rights under the GDPR, UK GDPR, Australian Privacy Act, Colombian Law 1581, Argentinian Law 25.326, and other applicable privacy laws. We implement appropriate technical and organizational safeguards for such data, including encryption, access controls, data minimization principles, and regular security assessments as required by various privacy laws including the Australian Privacy Principles (APPs), Colombian Law 1581, and Argentinian Law 25.326, and ensure compliance with all applicable data protection laws when processing special categories of personal data. For data processing under Swiss law, we implement additional safeguards required by the Swiss DPA, including specific measures for cross-border transfers, maintaining a record of processing activities (ROPA) as required by Article 12 of the Swiss DPA, implementing enhanced security measures for processing personality profiles, and ensuring compliance with the Swiss DPA's heightened transparency requirements for automated decision-making processes. We conduct regular data protection impact assessments (DPIAs) for high-risk processing activities involving sensitive personal data or personality profiles as required under Swiss law, and maintain documentation of our legal bases for processing such data in accordance with Article 6 of the Swiss DPA. We regularly review and update these safeguards to maintain their effectiveness and compliance with Swiss and other applicable data protection requirements.

Personal Information Sales Opt-Out and Opt-In

We will not sell, rent, lease, or otherwise transfer your personal information to third parties for monetary or other valuable consideration, and have not done so during the twelve (12) months preceding the effective date of this notice. We strictly prohibit the sale of personal information of minors under sixteen (16) years of age and have implemented technical and organizational measures to prevent such occurrences.

Your Rights Regarding Personal Information Sharing and Marketing

Pursuant to the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020 (collectively, the "CCPA"), California residents have certain rights regarding the "sharing" (as such term is defined in the CCPA) of their Personal Information with third parties for cross-contextual behavioral advertising purposes. Company does not engage in the sharing of Personal Information for cross-contextual behavioral advertising purposes and has not engaged in such sharing in the twelve (12) months preceding the effective date of this Privacy Notice. Furthermore, Company does not have actual

knowledge of any sharing of Personal Information of consumers under sixteen (16) years of age for cross-contextual behavioral advertising purposes.

We Will Not Discriminate Against You for Exercising Your Rights

We will not discriminate against you for exercising your rights under any applicable privacy law, including but not limited to the CCPA, GDPR, UK GDPR, Swiss FADP, PIPEDA (Canada), Privacy Act 1988 (Australia), Personal Data Protection Law (Argentina), Law 1581 (Colombia), and other relevant privacy regulations. Personnel will not be subject to any retaliation or disciplinary action for exercising their rights under the CCPA or any other applicable data privacy laws.

Exercising Your Rights Under Applicable Data Privacy Laws and International Data Transfers

To exercise the rights described in this Privacy Notice, you or your Authorized Agent (defined below) must send us a request that (1) provides sufficient information to allow us to verify that you are the person about whom we have collected personal information, and (2) describes your request in sufficient detail to allow us to understand, evaluate and respond to it. Each request that meets both of these criteria will be considered a "Valid Request." Acceptable verification methods vary by jurisdiction:

- For EU/UK residents: national ID cards, passport, or other official identification methods as permitted under the GDPR/UK GDPR

- For Swiss residents under FADP: Swiss ID card, passport, or other official identification

- For California and other US state residents: government-issued ID, utility bill, or account verification

- For Canadian residents under PIPEDA: government-issued ID or notarized statement

- For Australian residents: Australian government ID or proof of identity documents

- For Argentine residents: DNI or other official identification

- For Colombian residents: Cédula de Ciudadanía or other official identification

We may not respond to requests that do not meet these criteria. We will only use personal information provided in a Valid Request to verify your identity and complete your request. You do not need an account to submit a Valid Request.

We will work to respond to your Valid Request within the time period required by applicable law:

(i) For EU/UK residents: within 30 days, which may be extended by up to two additional months if necessary, given the complexity of the request;

(ii) For Swiss residents under FADP: within 30 days;

(iii) For California residents: within 45 days, which may be extended by an additional 45 days when reasonably necessary;

(iv) For Virginia, Colorado, Connecticut, and other US state residents: within 45 days, which may be extended by an additional 45 days when reasonably necessary;

(v) For Canadian residents under PIPEDA: within 30 days, which may be extended by up to 30 additional days if meeting the original deadline would unreasonably interfere with business activities;

(vi) For Australian residents: within 30 days;

(vii) For Argentine residents: within 10 working days for access requests and 5 working days for correction requests;

(viii) For Colombian residents: within 10 working days for requests related to personal data. We will inform you of any such extensions within the initial response timeframe, together with the reasons for the delay. We will not charge you a fee for making a Valid Request unless your Valid Request(s) is excessive, repetitive, or manifestly unfounded. This applies to all jurisdictions, including requests made under the GDPR, UK GDPR, CCPA, and other applicable privacy laws. If we determine that your Valid Request warrants a fee, we will notify you of the fee and explain that decision before completing your request.

You may submit a Valid Request using the following methods:

- https://privacy.x.ai/
- EU/UK Data Protection Officer: dpo@taceo.co.uk

You may authorize an agent (an "Authorized Agent") to exercise your rights on your behalf, subject to the following jurisdiction-specific requirements:

(a) For California residents (under CCPA/CPRA): Your Authorized Agent must (i) be registered with the California Secretary of State to conduct business in California; (ii) have written permission from you to submit request on your behalf; and (iii) verify their own identity with us. We may deny a request from an Authorized Agent who does not submit proof of authorization.

(b) For European Union residents (under GDPR): Your authorized representative must (i) be established in the European Union; (ii) have written mandate from you to act on your behalf; and (iii) comply with all applicable GDPR requirements for representatives. We reserve the right to verify the validity of the representative's mandate.

(c) For United Kingdom residents (under UK GDPR): Your authorized representative must (i) be established in the United Kingdom; (ii) have written mandate from you to act on your behalf; and (iii) comply with all applicable UK GDPR requirements for representatives.

For all jurisdictions, we may require additional verification steps and documentation to process requests from Authorized Agents to ensure the security and privacy of your information.

International Data Transfers

We transfer personal information to various countries outside your country of residence as follows:

1. European Union (EU) Transfers:
    - To the United States: We rely on our Intra-Group Data Processing Agreement which incorporates the EU Standard Contractual Clauses (SCCs) as approved by the European Commission within our group of companies, along with supplementary technical and organizational measures as required by the Schrems II decision. For transfers outside of our group of companies, we use the SCCs with appropriate supplementary measures.
    - To Canada: We rely on the European Commission's adequacy decision
    - To other non-adequate jurisdictions: We implement EU SCCs

2. United Kingdom (UK) Transfers:
    - To the United States: We use the UK International Data Transfer Agreement (IDTA)
    - To the EU/EEA: We rely on the UK's adequacy regulations for the EU/EEA
    - For transfers to countries without UK adequacy decisions: We use the UK International Data Transfer Agreement (IDTA)

3. Switzerland Transfers:
    - Standard Contractual Clauses with additional safeguards to address Swiss Federal Data Protection and Information Commissioner regarding government access to data.
    - To the EU/EEA: We rely on Swiss adequacy recognition

- To other non-adequate jurisdictions: We implement Swiss-approved SCCs

4. Other International Transfers:
    - For transfers from Asia-Pacific countries: We comply with APEC Cross-Border Privacy Rules (CBPR) where applicable
    - For transfers from Brazil: We implement SCCs adapted to LGPD requirements
    - For transfers from other jurisdictions: We implement appropriate safeguards as required by applicable local laws, including but not limited to specific requirements under Argentine Law 25.326, Colombian Law 1581 of 2012, and other applicable data protection regulations. For transfers from Argentina and Colombia, we obtain prior authorization from the respective data protection authorities where required by law.

Contact for Questions

If you have any questions or comments regarding this Privacy Notice, or wish to lodge a complaint with a supervisory authority (for EU/UK residents), or exercise your privacy rights under any applicable privacy law, the ways in which we collect and use your personal information or your choices and rights regarding such collection and use, please contact:

- https://privacy.x.ai/
- EU/UK Data Protection Officer: dpo@taceo.co.uk

Personnel with disabilities may access this Privacy Notice in an alternative format by contacting https://privacy.x.ai/.