OSACO
MAKE A DIFFERENCE

Privacy Policy for OSACO Group Incorporated HR & AI Guidance SaaS

Effective Date: 1 December 2025

1. Introduction This Privacy Policy describes how OSACO Group Incorporated ("we", "our", "us") collects, uses, and protects personal data in connection with our Human Resources (HR) support and AI guidance SaaS platform, also referred to as “EchoMind” ("Service"). We are committed to ensuring data privacy and compliance with applicable data protection laws, including the General Data Protection Regulation (“GDPR”) (*see* Endnotes 1 through 9).

2. Data Collection We collect and process the following categories of personal data:

- Personal identification information (e.g., name, email address)
- Employment details (e.g., job title, department)
- Usage data (e.g., interactions with the Service, device/browser information)
- Feedback and AI interaction logs

Data is collected directly from users, employers, and through our systems. We collect the above categories of personal information as defined under applicable U.S. state privacy laws, including identifiers, professional information, internet activity data, and inferences drawn from such data.

3. Purpose of Processing We process personal data for the following purposes:

- To provide and maintain the Service.
- To deliver HR-related support and AI-driven recommendations.
- To comply with legal obligations.
- To analyze usage and improve the Service.

We act as a service provider or processor on behalf of our clients with respect to employee and HR-related data. We process such data solely as instructed by our organizational clients.

4. Legal Basis for Processing We process data under the following lawful bases:

- Performance of a contract.
- Legitimate interests.
- Compliance with legal obligations.
- Consent (where required, e.g., for marketing or sensitive data).

In the U.S., we rely on contractual obligations and our role as a service provider to justify processing of HR-related personal data.

5. Data Sharing and Transfers We do not sell personal data. We may share it with:

- Service providers (e.g., cloud hosting, analytics).
- Legal authorities (when required).
- Subprocessors under binding agreements.

International data transfers are protected by appropriate safeguards such as Standard Contractual Clauses or participation in the EU-U.S. Data Privacy Framework. We do not sell or share personal information within the meaning of U.S. state privacy laws. When acting as a service provider, we limit use of personal data to client-authorized purposes only.

6. Automated Decision-Making and AI Use Our Service uses AI to provide recommendations and support. No legally significant decisions are made solely by automated means. Users may request human review of AI decisions and we continuously monitor system fairness and accuracy.

7. Data Retention We retain data only for as long as necessary for the specified purposes or as required by law. After this period, data is securely deleted or anonymized.

8. Data Subject Rights Under applicable laws, users may request:

- Access to their data.
- Rectification or erasure.
- Restriction or objection to processing.
- Data portability.

Any rights requests related to employee data must be directed to the employer (our client), as we act solely on their instructions.

Users may also lodge complaints with their national data protection authority.

9. Security Measures We employ technical and organizational security measures including:

- Encryption in transit and at rest.
- Role-based access controls.
- Regular security audits and monitoring.

9.1 Security Incidents

We implement measures to detect and respond to potential security incidents. In the event of a breach of security leading to the accidental or unlawful access to, disclosure of, or destruction of personal data, and where required by applicable law, we will notify affected individuals or our business clients without undue delay.

Not all security events constitute a breach requiring notification. We assess incidents on a case-by-case basis to determine whether notification obligations apply under relevant laws.

10. Data Breach Notification. In the event of any actual unauthorized access to or disclosure of Client Input Data or Personal Information in our possession or control (a "Security Incident"), we shall promptly notify Client without undue delay, and in no event later than seventy-two hours (72) after becoming aware of the Security Incident. Such notice shall include, to the extent known, the nature and scope of the breach, the types of data involved, and the steps taken or planned to mitigate and remediate the breach.

11. Changes to This Policy We may update this Privacy Policy from time to time. Users will be notified of material changes via the Service or by email.

For questions or concerns about this policy, please contact: [Insert contact details]

Endnotes – U.S. Privacy Law Citations

1. **California Consumer Privacy Act (CCPA), as amended by the CPRA**
   Cal. Civ. Code § 1798.100 et seq.
   Applicable to businesses that collect personal information from California residents and meet specific thresholds. Provides rights to know, delete, and opt-out of data sales.

2. **California Privacy Rights Act (CPRA)**
   Amends CCPA, effective Jan 1, 2023
   Expands rights under the CCPA and establishes the California Privacy Protection Agency.

3. **Colorado Privacy Act (CPA)**
   Colo. Rev. Stat. § 6-1-1301 et seq.
   Governs consumer rights and business obligations regarding personal data of Colorado residents.

4. **Virginia Consumer Data Protection Act (VCDPA)**
   Va. Code Ann. § 59.1-575 et seq.
   Establishes consumer rights and data controller responsibilities, including transparency and data minimization.

5. **Connecticut Data Privacy Act (CTDPA)**
   Public Act No. 22-15 (2022)

Mirrors provisions similar to VCDPA and CPA, focusing on transparency, consent, and consumer rights.

6. **Utah Consumer Privacy Act (UCPA)**
   Utah Code Ann. § 13-61-101 et seq.
   Applies to entities conducting business in Utah and processing personal data of residents.
7. **Health Insurance Portability and Accountability Act (HIPAA)**
   45 C.F.R. Parts 160 and 164
   If any employee health data is processed, this federal regulation may apply.
8. **Federal Trade Commission Act (FTC Act), Section 5**
   15 U.S.C. § 45
   Prohibits unfair or deceptive practices in commerce, including mishandling of personal data.
9. **Electronic Communications Privacy Act (ECPA)**
   18 U.S.C. § 2510 et seq.
   Regulates interception and disclosure of electronic communications, relevant to stored and transmitted data.
10. Criminal Justice Information Services (CJIS) Security Policy

    U.S. Department of Justice, Criminal Justice Information Services Security Policy, Version 5.5 (CJISD-ITS-DOC-08140-5.5) (June 1, 2016)

    Mandates comprehensive security measures for all agencies and organizations handling criminal justice information.