CCPA/CPRA Privacy Notice for Employees and Applicants

This Privacy Notice is made available pursuant to the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act of 2023 (CPRA).

Please review this notice carefully as it applies to the personal information, we collect about you solely in your capacity as a Tendo Systems Inc. **applicant, job candidate, employee, or former employee**.

Under the CCPA, personal information includes information that identifies and describes who you are, as well as information that relates to or is capable of being associated with, or could reasonably be linked to you, one of your devices, and/or a member of your household. In this Notice, we refer to the information subject to the CCPA as "Employee Personal Information."

You have the right to receive information on Tendo Systems Inc. privacy practices, including why we collect Employee Personal Information, from whom it is collected, and for what purpose.

Tendo Systems Inc. and its subsidiaries (together referred to here as "the Company"), collects and uses Employee Personal Information for human resources, employment, benefits administration, health and safety, and business-related purposes and to be in compliance with applicable statutes and regulations. Below are the categories of Employee Personal Information we collect and the purposes for which we intend to use this information.

The Company may collect the information below:

- **Identifying information,** such as your full name, gender, date of birth, and signature.
- **Demographic data**, such as race, ethnic origin, marital status, sexual orientation, disability, and veteran or military status.
- **Contact information**, such as your home address, telephone numbers, email addresses, and emergency contact information.

- **Dependent's or other individual's information**, such as their full name, address, date of birth, and Social Security numbers (SSN).
- **National identifiers**, such as SSN, passport and visa information, and immigration status and documentation.
- **Educational and professional backgrounds**, such as your work history, academic and professional qualifications, educational records, references, and interview notes.
- **Employment details**, such as your job title, position, hire dates, union membership, compensation, performance, and disciplinary records, and vacation and sick leave records.
- **Financial information**, such as banking details, tax information, payroll information, and withholdings.
- **Health and Safety information**, such as health conditions (if relevant to your employment), job restrictions, workplace illness, and injury information, and health insurance policy information.
- **Information Systems (IS) information**, such as your login credentials and information, search history, browsing history, and IP addresses on the Company's information systems and networks.
- **Biometric information**, such as facial recognition, fingerprints, iris or retina scans, keystrokes, or other physical patterns.
- **Geolocation data**, such as time and physical location related to the use of an internet website, application, device, or physical access to a Company office location.
- **Sensory or surveillance information**, such video surveillance in physical offices.
- **Profile or summary about an applicant or employee's preferences**, characteristics, attitudes, philosophical or religious beliefs, intelligence, abilities, and aptitudes.

The Company collects Employee Personal Information to use or disclose as appropriate to:

- Comply with all applicable laws and regulations.
- Recruit and evaluate job applicants and candidates for employment.

- Conduct background checks.
- Manage your employment relationship with us, including for:
    - onboarding processes.
    - timekeeping, payroll, and expense report administration.
    - employee benefits administration.
    - employee training and development requirements.
    - the creation, maintenance, and security of your online employee accounts.
    - reaching your emergency contacts when needed, such as when you are not reachable or are injured or ill.
    - workers' compensation claims management.
    - employee job performance, including goals and performance reviews, promotions, discipline, and termination; and
    - other human resources purposes.
- Manage and monitor employee access to company facilities, equipment, and systems.
- Conduct internal audits and workplace investigations.
- Investigate and enforce compliance with and potential breaches of Company policies and procedures.
- Engage in corporate transactions requiring review of employee records, such as for evaluating potential mergers and acquisitions of the Company.
- Maintain commercial insurance policies and coverages, including workers' compensation and other liability insurance.
- Perform workforce analytics, data analytics, and benchmarking.
- Administer and maintain the Company's operations, including for safety purposes.
- For client marketing purposes.
- Exercise or defend the legal rights of the Company and its employees, affiliates, customers, contractors, and or agents.

The Company collects Employee Personal Information by:

- Gathering from the applicant or job candidate themselves: either in person, by telephone, by email, or through systems that facilitate the collection of

information from you (e.g., the online administrative systems for employment applications, benefits, 401(k), and more).
- Access through publicly accessible sources (e.g., court records, social media sites, social networking sites).
- Directly from a third party (e.g., job boards, recruiters, screening providers, credit reporting agencies, or customer due diligence providers).
- Indirect or passive sources (e.g., cookies on our Sites; our IT systems; building security systems).

The Company may share Employee Personal Information with:

- Service providers the Company uses to help deliver benefits and services related to your prospective or actual employment, such as identity verification providers, payment service providers, time and attendance programs, benefits programs, and more.
- Third parties approved by you (e.g., your legal counsel, assessment and background check providers, and others).
- Law enforcement, government entities, and pursuant to the legal process where required by law.

The Company protects Employees' Personal Information:

Personal information is stored by the Company using industry-standard, reasonable, and technically feasible physical, technical, and administrative safeguards against foreseeable risks, such as unauthorized access.

Employees should be aware that the websites and data storage are run on software, hardware, and networks, any component of which may, from time to time, require maintenance or experience problems or breaches of security beyond the Company's control. The Company is not responsible for the acts and omissions of any third parties.

The Company cannot guarantee the security of the information on and sent from the Websites. No transmission of data over the internet is guaranteed to be completely secure. It may be possible for third parties not under the control of the Company to

intercept or access transmissions or private communications unlawfully. While we strive to protect your personal information, neither the Company nor any of our Service Providers can ensure or warrant the security of any information you transmit to us over the internet. Any such transmission is done at your own risk.

Retention and Sharing of Employee Personal Information:

The Company does not sell employee personal information and does not share such information with third parties for purposes of cross-context behavioral advertising. Employees, applicants, and job candidates will not be discriminated against for exercising their rights under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA).

The Company may collect and use employee personal information for business purposes related to employment, including but not limited to human resources, payroll, benefits administration, compliance, and IT security.

Unless a longer retention period is required or permitted by law, the Company retains all categories of employee personal information for a minimum of **six (6) years** following an employee's voluntary or involuntary separation from the Company. This retention period is intended to meet obligations under applicable employment, tax, benefits, and records retention laws, including but not limited to ERISA, the Internal Revenue Code, and relevant federal and state labor regulations.

Your Privacy Rights Under California Law

Under the California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), employees, applicants, and job candidates have the following rights regarding their personal information:

- The right to request deletion of personal information collected by the Company, subject to certain exceptions (e.g., when retention is necessary for

legal compliance, internal business purposes, or to fulfill the terms of employment).

- The right to know what personal information is being collected, used, shared, or sold, and to access that information.
- The right to correct inaccurate personal information.
- The right to limit the use and disclosure of certain sensitive personal information.
- The right to not be retaliated against for exercising any of these rights.

Employees with questions regarding the use and retention of Employee Personal Data or who would like to make a request to access, delete, or correct your personal information, or to exercise any other privacy rights, please contact Employee Success at hr@tendo.com