NEUTRAL PRIVACY NOTICE

1. PURPOSE

JAMS ("Company") respects Neutral privacy and is committed to protecting the Personal Information (defined below) it obtains and maintains. This policy provides Neutrals with notice and transparency; establishes guidelines for the Company to recognize and respect Neutral data privacy rights; and establishes guidelines to apply a consistently high level of protection to the Company's Processing (defined below) of Neutrals Personal Information.

2. SCOPE

This notice applies to current and former Neutrals. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time but if we do so, we will inform you and provide an updated copy of this notice on a central location.

3. OWNERSHIP

JAMS Legal owns and is responsible for updates, enforcement, and exceptions, and those may be appropriately delegated only to specified, qualified individuals. JAMS Legal is responsible for ensuring the policy is distributed and that all questions related to policy content are addressed.

4. DEFINITIONS

- **Associate** – includes individuals classified by the Company as full-time or part-time Associates.
- **Neutral** – includes individuals classified by the Company as full-time or part-time temporary neutrals or working on a limited service agreement providing ADR services in association with JAMS.
- **Information Systems** – hardware, software, technologies, networks, and systems used by the Company to conduct business or otherwise Process Personal Information or Sensitive Personal Information (defined below), including, but not limited to, any Third-Party electronic communications systems or remote computing services and related technology such as computing devices, cloud services, servers, websites, mobile devices, routers, email servers, messaging technologies, and social media platforms.
- **Personal Information ("PI")** – any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual. Examples include but are not

limited to personal unique identifiers such as full name and federal or state issued identification numbers; personal information such as telephone number and address and financial information; characteristics of protected classes under state or federal law; internet or other electronic network activity information; audio and visual information; employment information such as work history and prior employer, information from background checks, and resumes; education information such as student records and confirmation of graduation; and inferences based on information about an individual to create a summary about, for example, and individual's preferences and characteristics.

- PI does not include information that is publicly available or information that cannot be attributed to an individual because, for example, it has been aggregated with other information (e.g., statistical information) or otherwise de-identified in such a way that the Company cannot reasonably attribute the information to a specific individual.
- **Pseudonymized Information** should be considered personal information unless technical and organizational measures can ensure additional data points cannot be aggregated to re-identify an individual.
- **Sensitive Personal Information ("SPI")** – a subset of PI that carries more risk if it is exposed than PI. Examples include but are not limited to an individual's physical or mental health/condition; genetic and biometric data; precise geolocation; race/ethnicity; religious or philosophical beliefs; union membership; sexual activity or orientation; , social security, driver's license, state identification card, or passport number; contents of mail, email, and text messages unless the Company is the intended recipient of the communication; and 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.
- **Data Subject** – individuals from whom PI or SPI is collected or Processed.
- **Processing or Process** – any action performed on PI or SPI, including accessing, collecting, maintaining, recording, organizing, selling, structuring, storing, adapting, altering, retrieving, consulting, using, sharing, transmitting, combining with other data, restricting, or deleting PI or SPI. This definition includes any action performed on PI or SPI whether or not it is performed by an individual or individuals or by automated means.
- **Vendor** – any person or entity (other than an Associate) Processing Personal Information on behalf of the Company, including, but not limited to: a partner, vendor, supplier, third party, etc.

5. NOTICE

5.1. Types of Neutral Personal Information Processed

We collect, use, and store the following types of Personal Information about you:

Categories of Personal Information	Type of Personal Information
Identification data	• title • first name and last • date and place of birth • nationality • internal personnel number • photograph
Contact details (personal and professional)	• postal address • email address • telephone number • passport information • social security number
Information about your marital and family status	• family and marital status • dependents (name and date of birth) • contact details of individuals to contact in case of emergency
Professional data	• degrees, trainings, work experience, qualifications, references, information contained in your CV and/or cover letter • information collected during the recruitment process
Information necessary for the payment of your salary	• banking details
Information about your health	• data related to a disability • data related to accidents at work
CCTV images or any other information obtained electronically	• CCTV recordings • security badge and data related to the entry/exit from the building
Other data required to complete the hiring process	• the results of background checks

Information necessary for the administrative management of Neutral	• nature of the contract or commitment • place of work • start date with the company • seniority, position, and grade • HR records including job titles, department, work history, hours of work, information regarding the salary, leaves, compliance/training records and professional memberships • signed acknowledgements of Company Code of Conduct and policies • information on performance (including hours of work, financial performance data and evaluations) • results of any verification of employment status, details of your interest with any intermediary (for instance a company through which your services are provided) • information related to your use of IT and communication systems, including messages, emails, files, documents, or digital information • data related to training including your completed training classes and results • information related to disciplinary measures and grievances • separation date and reasons for your departure including any documents recorded or relevant to the departure such as the resignation letter

5.2. Use of Neutral Personal Information

Neutral Personal Information is collected and used for a range of standard business-related and business purposes, including:

- **Workforce Planning and Recruitment:** for example, for business forecasting, Associate assignment planning and budgeting, job advertising, interviewing, conducting background and criminal history checks, performing drug testing, selecting, and hiring and terminating staff.
- **General Human Resources Management and Administration:** for example, for career development, performance management, compensation and benefits management and benchmarking, administering payroll, reimbursing expenses, managing stock options, obtaining Associate satisfaction feedback, managing absences, general headcount reporting, disaster recovery and emergency response planning, equal opportunities monitoring, training Associates, and carrying out disciplinary or grievance procedures.
- **Performance of our Business Operations:** for example, to carry out day to day business activities, to allow us to work together and collaborate, to provide our services, to ensure business continuity, to enforce our rights and protect our

operations and those of our affiliates, and to pursue available remedies and limit damages we may sustain.

- **Security Management:** for example, to ensure the security of our premises, assets, information, and Associates.
- **Legal and Regulatory Compliance:** for example, to respond to law enforcement requests; as required by applicable law, court order, or governmental regulations; to ensure compliance with health & safety requirements and other legal or fiscal obligations, or in connection with litigation or an internal investigation or audit and to ensure compliance with our policies regarding anti- money laundering, bribery, and corruption.
- **Business transactions:** for example, to evaluate or conduct a merger, divestiture, restructuring, reorganization, dissolution, or other sale or transfer of some or all of the Company's assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal information held by the Company about you is among the assets transferred.
- **ANY OTHER PURPOSES As described to you** at the time your personal information is collected.

5.3. Disclosures of Neutral Personal Information

The Company may disclose your personal information as necessary for the purposes described in this Privacy Notice. For example, we may disclose your personal information the following parties:

- **Service Providers:** We use service providers to operate, host and facilitate our operations and business (including human resources operations). These include hosting, technology, and communication providers; security and fraud prevention consultants; analytics providers; background and reference check screening services; and hiring process and benefits management and administration tools.
- **Government authorities and law enforcement:** In certain situations, we may be required to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.
- **Business transfers:** Your personal information 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).
- **Professional advisors:** We may disclose your personal information with our professional advisors.
- **Other:** We may also disclose your personal information with third parties for purposes of fulfilling our legal obligations under applicable law, regulation, court order or other legal process, such as preventing, detecting, and investigating security incidents and potentially illegal or prohibited activities; protecting the rights, property, or safety of you, us, or another party; enforcing any agreements with you; responding to claims; and resolving disputes.

The Company does not sell your Personal Information. The Company does not share your Personal Information with third parties cross-context behavioral advertising. This includes your Sensitive Personal Information.

5.4. Your Rights

Under privacy and data protection laws, you have the following rights:

- Right to Know & Access the PI/SPI JAMS has collected about you, including the categories of PI/SPI, the categories of sources from which the PI/SPI is collected, the business or commercial purpose for collecting PI/SPI, the categories of third parties to whom JAMS discloses Candidate PI/SPI, and the specific pieces of PI/SPI JAMS has collected about you
- Right to Delete your PI/SPI, subject to certain exceptions
- Right to Correct inaccurate PI/SPI that JAMS maintains about you
- Right to Restrict JAMS' use of your PI/SPI
- Right to Data Portability of your PI/SPI in a structured, commonly used, and machine-readable format.
- Right to Non-Discrimination against you for exercising any of your rights.

JAMS does not Sell or Share your personal data; does not use automated decision making and profiling; and does not use or disclosure your Sensitive Personal Information for the purpose of inferring characteristics.

5.5. Neutral Personal Information Security and Retention

Neutral Personal Information is secured against unauthorized access or disclosure using reasonable and appropriate safeguards, in line with the Company's Information Security policy.

The Company retains Personal Information as long as reasonably necessary for its use and in accordance with applicable legal requirements.

6. POLICY MANAGEMENT

The Company reserves the right to amend the Neutral Privacy Notice at the Company's discretion and at any time. When we make changes to the Neutral Privacy Notice, we will post the updated notice on the JAMS Institute Library.
If you have any questions or concerns regarding this Privacy Notice or the collection and use of your Personal Information, please contact the Legal team.