ASM Global HR Customer Privacy Notice

Revised 12/22/2022 and effective 12/22/2022

INTRODUCTION

ASM Global Parent, Inc., on behalf of itself, its subsidiaries and affiliates (collectively, "ASM Global") is providing this ASM Global HR Customer Privacy Notice ("**HR Customer Privacy Notice**") to give its employees, job applicants, contractors (collectively "**Personnel**") and other individuals whose Personal Data (defined below) is collected for human resources purposes, information regarding how we collect and use your Personal Data for these purposes. In this Notice, "**Personal Data**" means data relating to identified or identifiable individuals and households.

SCOPE OF THIS POLICY

This HR Customer Privacy Notice applies only to Personal Data collected by ASM Global during the 12-month period preceding the effective date of this HR Customer Privacy Notice and used in the context of human resources, employment, and other internal business functions relating to our employees and their family members or beneficiaries, job applicants as well as independent contractors, including information collected and transmitted through internal computer systems, networks, and online services. ASM Global's Privacy Policy describes how ASM Global collects, uses and protects the Personal Data of consumers and users of ASM Global's services. To the extent ASM Global employees, job applicants and contractors engage with ASM Global as consumers outside of the employment context (such as if they purchase tickets to an ASM Global event) ASM Global's Privacy Policy would apply to the collection of Personal Data in connection with such a transaction.

CATEGORIES OF PERSONAL DATA

This chart describes the categories of Personal Data that ASM Global may collect in connection with its employment and contractual work relationships. Note, all Personal Data may be used and disclosed in connection with our Business Purposes.

Category of PI and Representative Data Elements	Context for Collecting and Sharing the PI
Contact Data • Honorifics and titles, preferred form of address • Mailing address • Email address • Telephone number • Mobile number • Social media or communications platform usernames or handles	We use your Contact Data to communicate with you by mail, email, telephone or text about your employment, including sending you work schedule information, compensation and benefits communications and other company information. Contact Data is also used to help us identify you and personalize our communications, such as by using your preferred name.
Identity Data • Full name, nicknames or previous names (such as maiden names) • Date of birth • Language • Company ID number • Company account identifiers and passwords • Benefits program identifiers • System identifiers (e.g., usernames or online credentials)	We use your Identity Data to identify you in our HR records and systems, to communicate with you (often using your Contact Data) and to facilitate our relationship with you, for internal record-keeping and reporting, including for data matching and analytics, and to track your use of company programs and assets, and for most processing purposes described in this HR Privacy Notice, including governmental reporting, employment/immigration verification, background checks, etc.
Government ID Data • Social security number • Driver's license number • Passport number • Other government-issued identifiers as may be needed for risk management or compliance (*e.g., if you are a licensed professional, we may collect your license number)*	We use your Government ID Data to identify you and to maintain the integrity of our HR records, enable employment verification and background screening, such as reference checks, license verifications, and criminal records checks, subject to applicable law, enable us to administer payroll and benefits programs and comply with applicable laws, such as reporting compensation to government agencies as required by law, as well as for security and risk management, such as collecting driver's license data for employees who operate company automobiles, professional license verification, fraud prevention and similar purposes. We may also use Government ID data for other customer business purposes, such as

	collecting passport data and secure flight information for employees who travel.
Biographical Data • Resume or CV • Data from LinkedIn profiles and similar platforms • Education and degree information • Professional licenses, certifications and memberships and affiliations • Personal and professional skills and talents summaries (e.g., languages spoken, CPR certification status, community service participation), interests and hobbies • Professional goals and interests	We use Biographical Data to help us understand our employees and for professional and personal development, to assess suitability for job roles, and to ensure a good fit between individuals' background and relevant job functions. We also use Biographical Data to foster a creative, diverse workforce, for coaching, and to guide our decisions about internal programs and service offerings.
Transaction and Interaction Data • Dates of Employment • Re-employment eligibility • Position, Title, Reporting Information • Work history information • Time and attendance records • Leave and absence records • Salary/Payroll records • Benefit plan records • Travel and expense records • Training plan records • Performance records and reviews • Disciplinary records	We use Transaction and Interaction Data as needed to manage the employment relationship and fulfill standard human resources functions, such as scheduling work, providing payroll and benefits and managing the workplace (e.g. employment creation, maintenance, evaluation, discipline, etc.).
Financial Data • Bank account number and details • Company-issued payment card information, including transaction records • Personal payment card information, if provided for reimbursement • Credit history, if a credit check is obtained (only done in limited circumstances)	We use your Financial Data to facilitate compensation, (such as for direct deposits), expense reimbursement, to process financial transactions, and for security and fraud prevention.
Health Data • Medical information for job placement, including drug testing and fitness to work examinations, accommodation of disabilities • Medical information for leave and absence management, emergency preparedness programs • Wellness program data • Information pertaining to enrollment and utilization of health and disability insurance programs	We use your Health Data as needed to provide health and wellness programs, including health insurance programs, and for internal risk management and analytics related to our human resources functions, staffing needs, and other Business Purposes.

Device/Network Data • Device information from devices that connect to our networks • System logs, including access logs and records of access attempts • Records from access control devices, such as badge readers • Information regarding use of IT systems and Internet access, including metadata and other technically-generated data • Records from technology monitoring programs, including suspicious activity alerts • Data relating to the use of communications systems and the content of those communications	We use Device/Network Data for system operation and administration, technology and asset management, information security incident detection, assessment, and mitigation and other cybersecurity purposes. We may also use this information to evaluate compliance with company policies. For example, we may use access logs to verify employee attendance records. Our service providers may use this information to operate systems and services on our behalf, and in connection with service analysis, improvement, or other similar purposes related to our business and HR functions.
Audio/Visual Data • Photograph • Video images, videoconference records • CCTV recordings • Call center recordings and call monitoring records • Voicemails	We may use Audio/Visual Data for general relationship purposes, such as call recordings used for training, coaching or quality control. We use CCTV recording for premises security purposes and loss prevention. We may also use this information to evaluate compliance with company policies. For example, we may use CCTV images to verify employee attendance records.
Inference Data • Performance reviews • Results of tests related to interests and aptitudes	We use inferred and derived data to help tailor professional development programs and to determine suitability for advancement or other positions. We may also analyze and aggregate data for workforce planning. Certain inference data may be collected in connection with information security functions, e.g. patterns of usage and cybersecurity risk.
Compliance and Demographic data • Diversity information • Employment eligibility verification records, background screening records, and other record maintained to demonstrate compliance with applicable laws, such as payroll tax laws, ADA, FMLA, ERISA *et al.* • Occupational safety records and worker's compensation program records • Records relating to internal investigations, including compliance hotline reports • Records of privacy and security incidents involving HR records, including any security breach notifications	We use Compliance and Demographic Data for internal governance, corporate ethics programs, institutional risk management, reporting, demonstrating compliance and accountability externally, to evaluate the diversity of our staff, and as needed for litigation and defense of claims.
Protected Category Data Characteristics of protected classifications under California or federal law, e.g. race, national origin, religion, gender, or sexual orientation.	We use Protected Category Data as needed to facilitate the employment relationship, for compliance and legal reporting obligations.

Sensitive Personal Information Social security, driver's license, state identification card, or passport number; account log-in and password, financial account, racial or ethnic origin, religious or philosophical beliefs, or union membership; mail, email, and text message content; biometric data for the purpose of uniquely identifying a natural person; data concerning health or data concerning a natural person's sex life or sexual orientation.	We use Sensitive Personal Information as needed to facilitate the employment relationship, determine company housing status, for compliance and legal reporting obligations. We may also use certain data regarding racial or ethnic origin for purposes related to various diversity, equity and inclusion initiatives., and we may sometimes share this information with third party partners.

SOURCES OF PERSONAL DATA

We collect Personal Data from various sources, which vary depending on the context in which we process that Personal Data.

- **Data you provide us** – We will receive your Personal Data when you provide them to us, when you apply for a job, complete forms, or otherwise direct information to us.
- **Data we collect automatically** – We may also collect information about or generated by any device you have used to access internal IT services, applications, and networks.
- **Data we receive from Service Providers** – We receive information from service providers performing services on our behalf.
- **Data we create or infer** – We (or third parties operating on our behalf) create and infer Personal Data such as Inference Data based on our observations or analysis of other Personal Data processed under this Privacy Notice, and we may correlate this data with other data we process about you. We may combine Personal Data about you that we receive from you and from third parties.

DISCLOSURE OF PERSONAL DATA

We generally process HR Personal Data internally; however, it may be shared or processed externally by third-party service providers to service employment, when required by law or necessary to complete a transaction, or in other circumstances described below.

CATEGORIES OF INTERNAL RECIPIENTS

The Personal Data identified below collected from our Personnel may be disclosed to the following categories of recipients in relevant contexts.

- **Personnel of HR Departments** – All Personal Data relating to Human Resources and Recruitment.
- **Personnel of Finance Departments** – Personal Data to the extent related to company and employee transactions
- **Direct Supervisors –** Elements of Personal Data to the extent permitted in jurisdiction, to the extent necessary to evaluate, establish, and maintain the employment relationship, conduct reviews, handle compliance obligations, and similar matters;
- **Department managers searching for new employees** – Personal data of job candidates contained in job applications to the extent allowed by relevant laws and departmental needs
- **Senior Supervisors –** Elements of Personal Data to the extent permitted in jurisdiction, to the extent necessary to evaluate, establish, and maintain the employment relationship, conduct reviews, handle compliance obligations, and similar matters.
- **IT Administrators** of ASM Global and/or third parties who support the management and administration of HR processes may receive Personal Data as necessary for providing relevant IT related support services (conducting IT security measures and IT support services)
- **Peers and colleagues –** Elements of Personal Data, to the extent permitted in jurisdiction, in connection with company address books, intracompany and interpersonal communications, and other contexts relevant to the day-to-day operation of company business.

CATEGORIES OF EXTERNAL RECIPIENTS

ASM Global may provide HR Personal Data to external third parties as described below. The specific information disclosed may vary depending on context, but will be limited to the extent reasonably appropriate given the purpose of processing and the reasonable requirements of the third party and ASM Global. We generally provide information to:

- Our parent company and other related entities.]
- Service providers, vendors, and similar data processors that process Personal Data on ASM Global's behalf (e.g., analytics companies, financial analysis/budgeting, trainings, benefits administration, payroll administration, etc.).
- To prospective seller or buyer of such business or assets in the event ASM Global sells or buys any business or assets.
- To future ASM Global affiliated entities, if ASM Global or substantially all of its assets are acquired by a third party, in which case Personal Data held by it about its employees will be one of the transferred assets.
- To government agencies or departments, employee unions, or similar parties in connection with employment related matters.
- To any public authority in relation to national security or law enforcement requests, if ASM Global is required to disclose Personal Data in response to lawful requests by public authority.
- To any other appropriate third party, if ASM Global is under a duty to disclose or share your Personal Data in order to comply with any legal obligation or to protect the rights, property, or safety of ASM Global, our employees, customers, or others.

LOCATIONS OF RECIPIENTS

ASM Global and some ASM Global affiliates are located in the United States, and some ASM Global subsidiaries and affiliates are located in other countries. Any Personal Data collected under this Policy from U.S. residents will likely be processed in the United States, however Personal Data may also be processed in other jurisdictions where ASM Global's parent company, affiliates and subsidiaries are located.

PURPOSES FOR COLLECTING, USING, AND DISCLOSING PERSONAL DATA

ASM Global collects Personal Data about its prospective, current, and former employees, job applicants, contractors and other individuals for various general HR and business purposes, as described below. We do not sell or share HR Personal Data with third parties in exchange for monetary consideration or for advertising purposes.

General HR Purposes

ASM Global collects Personal Data about its prospective, current, and former employees, job applicants, contractors and other individuals as appropriate in the context of an employment or contractual work relationship including for recruitment and IT/technical support services, and internal software, networks and devices. The categories of Personal Data we process, along with representative data elements, are listed in the chart below. We generally use, disclose and retain Personal Data processed under this HR Customer Privacy Notice for the following HR purposes:

Personal Data pertaining to ***prospective*** employees or contractors may be collected, used and shared for:	• Recruitment and staffing, including evaluation of skills and job placement, • Hiring decisions, including negotiation of compensation, benefits, relocation packages, *etc.*, • Determining an individual's eligibility to work and assisting with work permits or visas, • Risk management, including background checks, vetting and verification, and • ASM Global's Business Purposes (defined below).
Personal Data pertaining to ***current*** employees and contractors may be collected, used and shared for:	• Staffing and job placement, including scheduling and absence management, • Administration of compensation, insurance and benefits programs, • Time and attendance tracking, expense reimbursement, other workplace administration and facilitating relationships within ASM Global, • IT uses, such as managing our computers and other assets, providing email and other tools to our workers, • Diversity programs, • Health and wellness programs and accommodating disabilities, • Occupational health and safety programs (including required reporting, disaster and pandemic planning, and incident management), • Talent and performance development, skills management and training, performance reviews (including customer surveys), engagement surveys, and recognition and reward programs, • HR support services, such as responding to inquiries, providing information and assistance, and resolving disputes,

	• Risk management, including employee and premises monitoring (such as in our venues), or adjacent to ASM Global premises, • Providing employment and income verification (as requested by individuals), and • Business Purposes.
Personal Data pertaining to ***former*** employees and contractors may be collected, used and shared for:	• Re-employment, • Administration of compensation, insurance and benefits programs such as COBRA, • For archival and recordkeeping purposes, • Providing employment and income verification (as requested by individuals), and • ASM Global's Business Purposes.
Personal Data pertaining to individuals whose information is provided to ASM Global in the course of ***HR management*** (specifically beneficiaries, dependents, and emergency contact information pertaining to employees' family members) may be collected, used and shared for:	• Administration of compensation, insurance and benefit programs, • Workplace administration, • To comply with child support orders or garnishments, • To maintain internal directories, emergency contact lists and similar records, and • ASM Global's Business Purposes.

Business Purposes

"Business Purposes" means the following purposes for which Personal Data may be collected, used and shared:

- Identity and credential management, including identity verification and authentication, issuing ID card and badges, system administration and management of access credentials,
- Security, loss prevention, information security and cybersecurity,
- Legal and regulatory compliance, including without limitation, all uses and disclosures of Personal Data that are required by law or for compliance with legally mandated policies and procedures, such as anti-money laundering programs, security and incident response programs, intellectual property protection programs, and corporate ethics and compliance hotlines, and other processing in connection with the establishment and defense of legal claims,
- Corporate audit, analysis and consolidated reporting,
- To enforce our contracts and to protect ASM Global, its workers, its clients and their employees and the public against injury, theft, legal liability, fraud or abuse, to people or property,
- As needed to de-identify the data or create aggregated datasets, such as for consolidating reporting, research or analytics,
- Making back-up copies for business continuity and disaster recovery purposes, and other IT support, debugging, security, and operations.
- For the analysis and improvement of technical and organizational services, operations, and similar matters; and
- As needed to facilitate corporate governance, including mergers, acquisitions and divestitures.

DATA ADMINISTRATION

SECURITY

ASM Global requires that Personal Data be protected using technical, administrative, and physical safeguards, as described in our various security policies. ASM Global Personnel must follow the security procedures set out in applicable security policies at all times.

RETENTION AND DISPOSAL

ASM Global keeps Personal Data only for the amount of time it is needed to fulfill the legitimate business purpose for which it was collected or to satisfy a legal requirement. ASM Global Personnel must follow any applicable records retention schedules and policies and destroy any media containing Personal Data in accordance with applicable company policies.

YOUR CALIFORNIA PRIVACY RIGHTS

Under the California Consumer Privacy Act ("**CCPA**") and other comprehensive state privacy laws, residents of California may have the following rights, subject to your submission of an appropriately verified request (see the section "Verification of Requests" below for verification requirements):

Right to Know	You may request any of following, for the 12 month period preceding your request: (1) the categories of Personal Data we have collected about you, or that we have sold, or disclosed for a commercial purpose; (2) the categories of sources from which your Personal Data was collected; (3) the business or commercial purpose for which we collected, sold or shared your Personal Data; (4) the categories of third parties to whom we have sold or shared your Personal Data, or disclosed it for a business purpose; and (5) the specific pieces of Personal Data we have collected about you.
Right to Delete	You have the right to delete certain Personal Data that we hold about you, subject to exceptions under applicable law.
Right to Correct	You have the right to correct certain Personal Data that we hold about you, subject to exceptions under applicable law.
Right of Non-retaliation	You have the right to not to receive discriminatory treatment as a result of your exercise of rights conferred by the CCPA.
Direct Marketing	You may request a list of Personal Data we have disclosed about you to third parties for direct marketing purposes during the preceding calendar year, if applicable.

Verification of Requests

Requests to receive a copy of Personal Data, and requests to delete or correct Personal Data, must be verified to ensure that the individual making the request is authorized to make that request, to reduce fraud, and to ensure the security of your Personal Data. We may require that you log in through your ASM Global Workday account and/or that you provide the email address we have on file for you (and verify that you can access that email account) as well as other data we have on file, in order to verify your identity. If an agent is submitting the request on your behalf, we reserve the right to validate the agent's authority to act on your behalf.

CONTACT US / DATA INQUIRIES

If you are a current ASM Global employee with access to Workday, you can log in to your ASM Global Workday account to access, obtain copies of, delete, and correct certain Personal Data subject to this HR Privacy Notice. In addition, you may submit data requests via email to asmdataprivacy@asmglobal.com or by leaving a voicemail, along with requested Personal Data, at 1-844-919-1983, to the extent you have those rights under applicable law. You may also contact your HR Office for assistance. If you are a contractor without access to Workday, or an applicant, former employee or family member, or former contractor, please contact us at the address or email listed below for assistance with your privacy requests. For all other questions or comments about this HR Customer Privacy Notice or our privacy practices, please contact our Data Privacy Team:

Data Rights Requests: visit our privacy request page, call 1-844-919-1983, or mail to the address below,
Direct Marketing Disclosure Inquiries: mail to the address above or email asmdataprivacy@asmglobal.com
General Inquiries: asmdataprivacy@asmglobal.com

Please note that we do not sell Personal Data or share it for behavioral advertising purposes, so we do not offer the opportunity to opt out of such uses. Additionally, ASM Global does not use or disclose Sensitive Personal Information other than to provide you the Services and as permitted by California law. ASM Global does not sell or share Sensitive Personal Information for the purpose of cross-context behavioral advertising. Therefore, ASM Global does not provide a Notice of Right to Limit or provide a method for submitting a request to limit Sensitive Personal Information.

You may also reach our privacy team by mail:
ASM Global Parent, Inc.
Attn: Privacy
300 Conshohocken State Rd., Suite 770
West Conshohocken, PA 19428 (USA)