



## HYUNDAI AMERICA TECHNICAL CENTER, INC. (HATCI) JOB APPLICANT AND EMPLOYEE PRIVACY POLICY

**OVERVIEW:** Hyundai America Technical Center, Inc. (“HATCI”) and our parent company and affiliates (“Hyundai” “we,” “us” or “our”) are committed to privacy and transparency. This HATCI Privacy Policy (“Policy”) describes how we collect, use, disclose, and otherwise process the personal information described in this Privacy Policy related to our job applicants (“Applicants”) and employees, independent contractors, interns, consultants, and other individuals who interact with HATCI in an employment-related capacity (collectively, “Employees”), as well as the rights and choices individuals have regarding such personal information. This Policy generally refers to employees and employee data, but this does not in any way indicate that an individual is our employee, it does not form any contract of employment, and it does not modify the employment terms of any candidates hired by HATCI.

**PURPOSE OF THE POLICY:** This Policy is also intended to satisfy our applicable notice requirements under the California Consumer Privacy Act (“CCPA”) (as amended by the California Privacy Rights Act of 2020 (“CPRA”), codified at Cal. Civ. Code § § 1798.100–1798.199.100 and the California Consumer Privacy Act Regulations issued thereto, Cal. Code Regs. tit. 11, div. 6, ch. 1). We may provide Applicants additional notices about our data collection practices that are covered by other laws (e.g., if we conduct a background check or extend an employment offer).

**SCOPE OF THE POLICY:** This Policy applies to the personal information that we collect and use in order to manage the limited relationship we have with our Applicants. This Policy also applies to the personal information we collect from Employees, and other individuals whose information we collect in connection with providing employment such as emergency contacts, beneficiaries, and dependents. It does not apply to protected health information, publicly available information (as defined by the CCPA), consumer credit reports and background checks, publicly available data lawfully made available from state or federal government records, or other information that is exempt under the CCPA.

**CATEGORIES OF PERSONAL INFORMATION COLLECTED AND DISCLOSED:** While the categories of personal information that we collect and our use of such personal information may vary depending on the position or location for which you apply or are employed, generally we may collect and have in the past twelve months collected the following categories of personal information about you and disclose it to certain parties as described below:

| Category   | To Whom We May Disclose this Information   |
|--|--|
| <p><b>Name, Contact Information, and Other Identifiers.</b><br/>Identifiers such as a real name, alias, postal address, email address, phone number, social security number, driver’s license number, passport number, photograph, signature, or other similar identifiers.</p>  | <ul style="list-style-type: none"> <li>▪ Parent company and affiliates</li> <li>▪ Service providers and suppliers (as needed)</li> <li>▪ Government entities and law enforcement (as needed/upon request)</li> </ul> |
| <p><b>Protected Classifications.</b> Characteristics of protected classifications under California or federal law such as race, color, sex, sexual orientation, gender identity, gender expression, age, religion, national origin, disability, citizenship status, military/veteran status, marital status, and medical conditions.</p>   | <ul style="list-style-type: none"> <li>▪ Parent company and affiliates</li> <li>▪ Service providers and suppliers (as needed)</li> <li>▪ Government entities and law enforcement (as needed/upon request)</li> </ul> |
| <p><b>Usage Data.</b> Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding your interaction with an internet website or application.</p>  | <ul style="list-style-type: none"> <li>▪ Parent company and affiliates</li> <li>▪ Service providers and suppliers (as needed)</li> <li>▪ Government entities and law enforcement (as needed/upon request)</li> </ul> |
| <p><b>Audio/Visual.</b> Audio, electronic, visual, or similar information, such as, CCTV footage, photographs, and audio recordings (e.g., recorded meetings and webinars).</p>  | <ul style="list-style-type: none"> <li>▪ Parent company and affiliates</li> <li>▪ Service providers and suppliers (as needed)</li> <li>▪ Government entities and law enforcement (as needed/upon request)</li> </ul> |
| <p><b>Professional and Employment Information.</b> Professional or employment-related information including position, title, job description, department, contract details (if any), resume, recruitment history, application form, compensation and benefits information (e.g., salary-related information, tax-related information, benefits elections, payroll deductions, and details regarding leaves of absence), disciplinary information, such as employee misconduct or misbehavior, evaluation records, performance assessments and performance reviews, academic background, such as education history, transcripts, certificates, professional associations, historic compensation details, previous employment details, and pre-employment screenings and background checks, including criminal records</p> | <ul style="list-style-type: none"> <li>▪ Parent company and affiliates</li> <li>▪ Service providers and suppliers (as needed)</li> <li>▪ Government entities and law enforcement (as needed/upon request)</li> </ul> |

|   |  |
|---|--|
| information, drug-screening results, emergency contact information, marital status, dependent and beneficiary information, and securities holding information.  |  |
| <b>Non-Public Education Information.</b> Information about education history or background that is not publicly available personally identifiable information as defined in the federal Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99).   | <ul style="list-style-type: none"> <li>▪ Parent company and affiliates</li> <li>▪ Service providers and suppliers (as needed)</li> <li>▪ Government entities and law enforcement (as needed/upon request)</li> </ul> |
| <b>Profiles and Inferences.</b> Inferences drawn from any of the information identified above to create a profile about an Applicant or Employee reflecting the Applicants or Employees preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.   | <ul style="list-style-type: none"> <li>▪ Parent company and affiliates</li> <li>▪ Service providers and suppliers (as needed)</li> <li>▪ Government entities and law enforcement (as needed/upon request)</li> </ul> |
| <b>Sensitive Personal Information.</b> Social security number, driver’s license number, motor vehicle report (driving record), financial account information, insurance policy number(s), state identification number, passport number, biometric information, medical conditions, drug-screening results, race, national origin, religious beliefs, sexual orientation, and gender identity. | <ul style="list-style-type: none"> <li>▪ Parent company and affiliates</li> <li>▪ Service providers and suppliers (as needed)</li> <li>▪ Government entities and law enforcement (as needed/upon request)</li> </ul> |

**PURPOSES FOR COLLECTING AND USING PERSONAL INFORMATION:** Generally, we may use the above categories of personal information for the following business purposes:

|   |
|---|
| <p><b>Recruiting, Evaluating, Hiring, and Managing Job Applicants.</b> To review, assess, recruit, consider, or otherwise manage Applicants and job applications, including:</p> <ul style="list-style-type: none"> <li>• Scheduling and conducting interviews.</li> <li>• Identifying applicants, including by working with external recruiters as needed.</li> <li>• Reviewing, assessing, and verifying information provided.</li> <li>• Conducting criminal and background checks (where relevant and pursuant to applicable law), and to otherwise screen or evaluate applicants’ qualifications, suitability, and relevant characteristics.</li> <li>• Extending offers, negotiating the terms of offers, and assessing salary and compensation matters.</li> <li>• Satisfying legal and regulatory obligations.</li> <li>• Accommodating disabilities.</li> <li>• Verifying eligibility to work in the U.S.</li> <li>• Communicating with applicants regarding their applications and about other similar position(s) for which they may be interested.</li> </ul> |
|---|

- Maintaining applicant personal information for future consideration.
- Supporting our equal opportunity employment policy and practices.

**Managing and Evaluating Employees.** To review, assess, monitor, and otherwise manage Employees, including:

- Conducting performance related reviews including performance appraisals, career planning, skill monitoring, job duties, promotions, and staff restructure.
- Assessing ability, fitness, or eligibility to perform job duties or work.
- Providing Employees with Human Resources management including employee data maintenance and support services, separation and termination of employment, approvals and authorization procedures, administration and handling of employee claims, and travel administration.
- Verifying and monitoring eligibility to work in the U.S. and ensuring compliance with related laws and regulations.
- Applying for U.S. immigration benefits.
- Accommodating disabilities or illness.
- Administering and providing compensation, including payroll, bonus, and other applicable incentives.
- Administering and providing applicable benefits and work-related allowances, including insurance, 401K, cell phones, laptops, and the corporate vehicle program.
- Maintaining contact and emergency contact information.
- Supporting our equal opportunity employment policy and practices.
- Assisting in case of emergency.

**Security and Monitoring.** To monitor and secure our resources, network, premises, and assets, including:

- Grant and monitor access to secure company facilities.
- Monitoring for, preventing, and investigating suspected or alleged misconduct or violations of work rules.
- Monitoring for, preventing, investigating, and responding to security and privacy incidents.
- Providing and managing access to physical and technical access controls.
- Monitoring activities, access, and use to ensure the security and functioning of our systems and assets.
- Securing our offices, premises, and physical assets, including through the use of electronic access systems and video monitoring (as applicable).

**Auditing, Accounting and Corporate Governance.** Relating to financial, tax and accounting audits, and audits and assessments of our business operations, security controls, financial controls, or compliance with legal obligations, and for other internal business purposes such as administration of our records retention program.

**Business Transactions.** For purposes of planning, due diligence, and implementation of commercial transactions (e.g., mergers, acquisitions, asset sales or transfers, bankruptcy or reorganization or other similar business transactions, as applicable).

**Defending and Protecting Rights.** To protect and defend our rights and interests and those of third parties, including to manage and respond to legal claims or disputes, and to otherwise establish, defend or protect our rights or interests, or the rights, interests, health or safety of others, including in the context of anticipated or actual litigation with third parties.

**Compliance with Applicable Legal Obligations.** Relating to compliance with applicable legal obligations (such as hiring eligibility, responding to subpoenas and court orders) as well as assessments, reviews, and reporting relating to such legal obligations, including under employment and labor laws and regulations, social security and tax laws, environmental regulations, workplace safety laws and regulations, immigration regulations, and other applicable laws, regulations, opinions, and guidance.

We do not sell or share Applicant or Employee personal information, including sensitive personal information, with third parties based on the definitions of sell and share in the CCPA and we have not sold or shared in the past twelve months.

**SOURCES OF PERSONAL INFORMATION:** We collect information that you give us directly when you apply for a job, complete your employment paperwork during the onboarding process, enroll in company benefits, or when you otherwise interact with us and provide personal information in the context of your job application or employment. This includes information about Employee’s beneficiaries and dependents. We may collect information about you from third parties (such as prior employers or professional references) and our service providers to whom you provide your personal information (such as recruiters or employee benefits providers).

**RETENTION OF PERSONAL INFORMATION:** We will retain your personal information, including sensitive personal information, as long as necessary for purposes for which the personal information was collected and is used by us, as stated in this Policy. In general, with respect to categories of personal and sensitive information of Applicants, we retain each category until the withdrawal or rejection of your application. In general, with respect to categories of personal and sensitive information of Employees, we retain each category until the end of your employment, plus four years and any additional time periods necessary for the compliance with laws, exercise or defense of legal rights, and archiving, back-up, and deletion processes.

**SENSITIVE PERSONAL INFORMATION:** We collect and use certain sensitive personal information which may vary depending on the circumstances. We may collect the following categories of sensitive personal information, as indicated in the “Categories of Personal Information Collected” section above.

Notwithstanding the “Purposes for Collecting and Using Personal Information” section above, we only use or disclose sensitive personal information as reasonably necessary (i) to perform services requested by you, (ii) to help ensure security and integrity, including to prevent, detect, and investigate security incidents, (iii) to detect, prevent, and respond to malicious, fraudulent, deceptive, or illegal conduct, (iv) to verify or maintain the quality and

safety of our services, (v) for compliance with our legal obligations, (vi) to our service providers who perform services on our behalf, and (vii) for other purposes other than inferring characteristics about you. We do not use or disclose your sensitive personal information other than as authorized pursuant to the CCPA.

**JOB APPLICANT AND EMPLOYEE RIGHTS:** In general, Applicants and Employees have the following rights with respect to their personal information:

- **Do not sell or share (opt-out):** The right to opt-out of our sale or sharing of your personal information.
- **Right of deletion:** The right to request deletion of their personal information that we have collected and to have such personal information deleted (without charge), subject to certain exceptions.
- **Right to know:** The right to know the following about how we have handled your personal information:
  - Categories of personal information collected;
  - Specific pieces of personal information collected;
  - Categories of sources of personal information;
  - Categories of personal information about them we have disclosed for a business purpose or sold;
  - Categories of third parties to whom we have disclosed for a business purpose your personal information;
  - Categories of personal information sold or shared and categories of third parties to whom the personal information was sold or shared;
  - The business or commercial purposes for collecting, selling, or sharing personal information; and
  - A copy of the specific pieces of personal information we have collected about you.
- **Right to correct inaccurate information:** The right to request correction of your personal information that we have collected about you and to have such personal information corrected.
- **Right to limit the use or disclosure of sensitive personal information:** With respect to sensitive personal information, the right to require we limit our use or disclosure of sensitive personal information to those uses authorized by the CCPA. However, we do not use or disclose sensitive personal information except for the purposes described above under “Sensitive Personal Information,” as authorized by the CCPA.
- **Right to non-discrimination:** The right not to be subject to discriminatory treatment for exercising your rights under the CCPA. We will not discriminate against you for exercising your rights.

**SUBMITTING REQUESTS:** To exercise the rights described above, you may submit a request via email to [legal\\_help@hatci.com](mailto:legal_help@hatci.com), by calling (734) 337-2500, or via U.S. mail to:



Hyundai America Technical Center, Inc.  
ATTN: Nicholas Sulla, General Counsel  
6800 Geddes Road  
Superior Township, MI 48198

In order to make a verifiable request, you must provide sufficient information to allow us to verify you are the person about whom we collected personal information. We cannot respond to your request or provide you with personal information if we cannot verify your identity or authority to make the request and confirm the personal information relates to you. We will only use personal information provided in a request to verify the requestor's identity or authority to make the request. Only you or your authorized agent may make a verifiable request related to your personal information. If you use an authorized agent to submit a request on your behalf, we may require that you provide 1) a copy of written permission for the authorized agent to make the request and/or 2) a copy of a power of attorney that complies with the law. You may only make a verifiable request twice within a twelve-month period.

You must also describe your request with sufficient detail that allows us to properly understand, evaluate, and respond to it. We will respond to a request within 45 days of its receipt. If we require more time (up to 45 additional days for a total of 90 days from receipt of the request), we will inform you in writing. We will deliver our written response by mail or electronically. There may be circumstances where we will not be able to honor your request. For example, if you request deletion, we may need to retain certain personal information to comply with our legal obligations or other permitted purposes. The response will explain the reasons we cannot comply with a request, if applicable.

**CONTACTING US ABOUT THIS POLICY:** If you have any questions or concerns regarding our use of personal information as described in this Policy, please contact [legal\\_help@hatci.com](mailto:legal_help@hatci.com).

**ACCESSIBILITY:** We are committed to ensuring this Policy is accessible to individuals with disabilities. If you wish to access this Policy in an alternative format, please contact [legal\\_help@hatci.com](mailto:legal_help@hatci.com).

**UPDATES:** HATCI reserves the right to change this Policy at any time. This Policy may be updated to reflect changes in our business, legal, or regulatory obligations so please check this Policy periodically for changes.