

# **PRIVACY NOTICE FOR TRANSDIGM GROUP INCORPORATED**

## **CALIFORNIA PERSONNEL**

Effective Date: May 24, 2024

Last Updated: May 24, 2024

TransDigm Group Incorporated together with its subsidiaries and affiliates (collectively, "Company", "us," "we," or "our") is committed to protecting the privacy of Personal Data (defined below). This Privacy Notice for Company California Personnel (this "Privacy Notice") informs you of our practices concerning the processing of California residents' Personal Data collected through online and offline interactions while you are working for us and after you have left. It applies to current and former full-time, part-time, or temporary employees (and their dependents) and contractors who are California residents (together referred to as "Personnel" or "you"). If you interact with our website, purchase our products or services, or otherwise engage with us outside of your employment relationship, the TransDigm Group Incorporated Privacy Policy applies to any Personal Data we process through those interactions, not this Privacy Notice.

We are required by California's privacy laws and regulations to give you the information in this Privacy Notice. It is important that you read this Privacy Notice carefully, together with any other information that we might give you from time to time about how we collect and use your Personal Data.

Whenever you interact with us on behalf of another individual or entity, such as if you provide information about a dependent, you must obtain their consent (or have the legal authority without consent) to share their Personal Data with us.

**Changes:** We may update this Privacy Notice from time to time. Any updated Privacy Notice will be effective when posted on <http://www.trandigm.com>. Please check this Privacy Notice periodically for updates. If required by law, we will contact you directly to provide you with an updated Privacy Notice.

This Privacy Notice does not form part of any contract of employment or other contract to provide services and does not give you any contractual rights.

### **1. Sources of Personal Data**

"Personal Data" is any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with you or your household as and to the extent provided by applicable California 55law.

We collect Personal Data about you from the following sources:

**A. Directly from you.** We may collect Personal Data you provide to us directly, such as information provided to establish our employment relationship, when you register for benefits and through your daily interactions with us during your employment.

**B. Data collected automatically and through tracking technologies.** We may automatically collect information or inferences about you (including as part of our insider threat initiatives), such as through tracking technologies. This may include information about how you

browse the Internet and use Company's devices and the content of sent and received emails where we are permitted to collect such information under applicable law.

**C. From third parties.** We may collect Personal Data from third parties, such as companies that provide benefits, payroll, travel, or other services, and from publicly available sources, such as LinkedIn. We may also receive Personal Data from your colleagues or supervisors, for example, in the context of performance evaluations.

We may combine and use information and make inferences from information that we receive from the various sources described in this Privacy Notice, including third-party sources. We also use or disclose the combined information and inferences for the purposes identified below.

## **2. Types of Personal Data We Collect**

We may collect the following types of Personal Data about you and your family members, such as spouses, partners, children, dependents, beneficiaries, or parents, as applicable:

**A. Identifiers**, such as name, alias, photograph, email address, physical address, telephone number, business contact information, device identifiers (e.g., IP address, cookies, beacons, pixel tags, mobile ad identifiers and similar technology), online identifiers, and other similar identifiers.

**B. Personal Data described in subdivision (e) of Cal. Civ. Code § 1798.80**, such as

1. nationality;
2. place of birth;
3. civil/marital status;
4. emergency contact and next of kin information;
5. signatures; and
6. your physical characteristics or a description of you.

**C. Protected classifications under California or federal law**, such as age (including birthdates), military or veteran status, marital status, citizenship status, and gender.

**D. Commercial information**, such as records of business transactions, bank account details and tax status, credit-related information, bonus stock options and other incentives, shareholder information, financial interest in our customers, and student loan contributions.

**E. Biometric information**, such as fingerprints, face recordings, and voice recordings.

**F. Internet or other electronic network activity information**, such as information relating to your access to and use of or interactions with Company facilities, network systems, devices, email, applications, and platforms, including your browsing history, search history, information regarding interactions with and use of Internet websites and applications, and the content of communications and information processed within global digital communication platforms, to the extent permitted under applicable law.

**G. Non-precise geolocation data**, such as your location as derived from your IP address.

**H. Audio, electronic, visual, or other sensory information**, such as photographs or security camera footage in public areas of Company's facilities (including reception, the work floor, conference rooms, parking, and other general areas), and as collected in the course of training events, meetings, videoconferences, and other events that we or you may organize that may be photographed or recorded.

**I. Professional or employment-related information**, such as job title, organization, business unit/department and its location, start and termination dates and termination reasons, information on assigned company devices/credit card numbers/cars (if any), contract details, personal characteristics (such as hobbies and interests), work planning, professional certifications and licenses, credentials, professional specialties and other relevant skills and achievements, professional affiliations, professional experience, timekeeper records, working hours, training records, professional memberships, dedicated identifiers (e.g., employee ID, badge), references, performance and other evaluation information, disciplinary information, resumes, cover letters, interview notes, human resources records, compensation history, payroll and benefits data (including for dependents), overtime pay, pension administration and pension qualification information, attendance/working time records, leave records, wellness information, board of directors appointments, right to work documentation, titles, languages, profile information on professional networking platforms, information related to meetings (such as information available on platforms you use to organize and participate in meetings), work travel information, and any other information you may provide in connection with your employment (such as through a hotline). In addition, we may collect information about criminal convictions and offenses, information collected as part of internal investigations or disciplinary or legal proceedings, and information from background checks.

**J. Education Information**, such as education history and grades, professional qualifications, academic certificates and licenses, languages spoken, and other relevant skills.

**K. Inferences** drawn from any of the information identified in this Section 2, such as software used to review activity on Company systems, networks, or email to evaluate insider threats, and information used to evaluate performance.

**L. Sensitive Personal Data**, potentially including the following:

1. Social Security number, driver's license, state identification card, or passport number.
2. Account log-in details including any required security or access code, password, or credentials allowing access to an account.
3. Precise geolocation.
4. Racial or ethnic origin, or religious or philosophical beliefs, if you choose to provide them.
5. Content of mail, email, and text messages where we are not the intended recipient (such as the content of emails you send to third parties, which may include personal emails sent using your Company email address).

6. Information about your health, including medical conditions, health and sickness records, vaccination status, disabilities, maternity records, incident/accident information involving health data, whether you were exposed to someone who tested positive for communicable diseases or whether you are currently experiencing any flu-like or other relevant symptoms, and information about your health insurance, including insurance policy number.

7. Information you choose to provide concerning your sexual orientation.

### 3. **How we Use Personal Data**

We may use Personal Data for the following purposes:

**A. Human resources management**, such as verifying your identity; determining eligibility for benefits; administering payroll and benefits (including sickness, parental, adoption and bereavement leave, pensions, government-related programs, stock and equity plans, and death-in-service programs); logistics; planning and managing corporate travel and other reimbursable expenses; development and training; absence monitoring; timekeeping; performance appraisals; disciplinary and grievance processes; administration of termination of employment; career planning; administration of relocation; assessing qualifications and eligibility for a particular role or project; right to work requirements; diversity and inclusion surveys and other activities (including to understand make up and representation in the workforce, for pay gap initiatives, and to allow us to offer support to certain demographic groups); background checks and reference checks; alumni programs to stay in touch with former Personnel; and complaint/hotline programs. In addition, we may use your Personal Data to respond to customer inquiries about the demographics of our employees or to include your information in the diverse employee directory for staffing and business development purposes in accordance with your consent.

**B. For our internal business purposes**, such as enforcing our policies and rules; organizational analysis; management reporting; managing Company assets and our workforce; work planning, both administratively and organizationally (including work scheduling and billing customers); provide requested information about our products or services, email alerts, and event registration; provide services to our customers; project management; auditing; maintaining records on business activities (such as accounting and commercial activities); document management and similar activities; budgeting; real estate management; IT administration of our technologies, network, and intranet; IT security management and tasks; analyzing and managing meeting information (including, but not limited to, recording content, conversations and discussions, which may include your voice and/or images in case of video conferences, trainings, meetings, and other events); documenting corporate decision-making processes; making online event available to our Personnel for training purposes and/or to allow them or our partners to review such events after they have finished; maintaining benchmark statistical information; helping Personnel improve meeting management; increasing meeting productivity; optimizing meeting resource distribution; and providing insights into interactions with people you network with.

**C. For our internal research and product improvement purposes**, such as verifying or maintaining the quality or safety of our products or services, including website content; improving our products and services; designing new products and services; and debugging and repairing errors with our systems, networks, and equipment.

**D. For legal, safety or security reasons**, such as complying with legal and contractual requirements; complying with reporting and similar requirements; conducting compliance training; investigating and responding to claims against Company, its customers, or its Personnel; completing due diligence (such as in connection with a corporate transaction); equal opportunity monitoring and compliance; environmental, health, and safety purposes; maintaining medical and sickness records and occupational health programs; keeping emergency contacts; behavioral safety purposes; detecting, preventing, and responding to security, health and safety incidents; ascertaining your fitness for work; protecting the rights, health, and safety of Personnel and others, including by preventing or reducing the spread of communicable diseases in the workplace; receiving legal advice or approval; and, protecting against cyberattacks, identify theft, malicious, deceptive, fraudulent, or illegal activity.

**E. Workplace monitoring**, such as controlling and monitoring Company's facilities (through, e.g., use of surveillance cameras or other methods of identification and monitoring); using systems, applications, records and equipment to protect individuals and property; recording telephone conversations; monitoring email, Internet, device, vehicle, and other asset usage; time clock recording; ensuring compliance with internal policies and practices; maintaining global/entity-wide digital communication and data sharing/storage platforms; investigating unauthorized use, access, logs or theft of property or Personal Data breaches; and providing IT support to Personnel.

**F. In connection with a corporate transaction**, such as if we acquire, or some or all of our assets are acquired by, another entity, including through a sale in connection with bankruptcy and other forms of corporate change.

**G. For marketing**, including externally promoting Company and our brands, goods, and services. We may do so via social media, through public relations materials and communications, reputation and business-development efforts, branding, at events, and directly to customers or potential customers. For example, we may provide business partners with the names and work contact information of account representatives or post pictures of Personnel who attend public Company events. We do not use Sensitive Personal Data for such purposes.

We only use Sensitive Personal Data for the following purposes: (i) performing services or providing goods reasonably expected by an average consumer; (ii) detecting security incidents; (iii) resisting malicious, deceptive, or illegal actions; (iv) ensuring the physical safety of individuals; (v) for short-term, transient use, including non-personalized advertising; (vi) performing or providing internal business services; (vii) verifying or maintaining the quality or safety of a service or device; or (viii) for purposes that do not infer characteristics about you.

We may use anonymized, de-identified, or aggregated information for any purpose.

#### **4. How and to Whom We Disclose Personal Data**

We may disclose Personal Data to third parties, including the categories of recipients described below:

**A. Affiliates and subsidiaries**, including parent entities, corporate affiliates, subsidiaries, business units, and other companies that share common ownership with us.

**B. Service providers** that work on our behalf to provide products and services, such as providers of the following services: IT, payroll management, recruitment, networking, onboarding, learning and training delivery and management, email, mailing and printing, maintenance/facilities

management, confidential waste management, access control and monitoring solutions, internal communication channels, data analytics, helpdesk platform, and workforce assessment, among others.

**C. Benefits and other financial services providers**, such as health and medical insurance providers and providers of retirement savings and other financial services.

**D. Professional consultants**, such as accountants, lawyers, financial advisors, and audit firms.

**E. Vendors necessary to complete transactions you request**, such as shipping companies, couriers, and logistics providers.

**F. Law enforcement, government agencies, and other recipients for legal, security, or safety purposes**, such as when we share information to comply with law or legal requirements, to enforce or apply our policies, and to protect our, our customers', or third parties' safety, property, or rights.

**G. To other entities in connection with a corporate transaction**, such as if we, or some or all our assets, are acquired by another entity, including through a sale in connection with bankruptcy or other forms of corporate change.

**H. Entities to which you have consented to the disclosure**, where consent is required by law.

**5. Additional Disclosures**

We do not sell or share Personnel Personal Data.

Below please find a chart detailing the categories of Personal Data and with whom it was disclosed for a business purpose in the past 12 months:

<i>Categories of Personal Data We Collect</i>	<i>Categories of Third Parties With Whom We Disclose Personal Data for a Business Purpose</i>
<b>Identifiers</b> (Section 2.A)	<ul style="list-style-type: none"> <li>• Affiliates and subsidiaries</li> <li>• Service providers</li> <li>• Benefits and other financial services providers</li> <li>• Professional consultants</li> <li>• Vendors necessary to complete transactions you request</li> <li>• Recipients for legal, security, or safety purposes</li> <li>• In connection with a corporate transaction</li> <li>• Entities to which you have consented to the disclosure</li> </ul>
	<ul style="list-style-type: none"> <li>• Affiliates and subsidiaries</li> <li>• Service providers</li> <li>• Benefits and other financial services providers</li> </ul>

<p><b>Personal Data described in subdivision (e) of Cal. Civ. Code § 1798.80</b></p> <p>(Section 2.B)</p>	<ul style="list-style-type: none"> <li>• Professional consultants</li> <li>• Vendors necessary to complete transactions you request</li> <li>• Recipients for legal, security, or safety purposes</li> <li>• In connection with a corporate transaction</li> <li>• Entities to which you have consented to the disclosure</li> </ul>
<p><b>Characteristics of protected classifications under California or federal law</b></p> <p>(Section 2.C)</p>	<ul style="list-style-type: none"> <li>• Affiliates and subsidiaries</li> <li>• Service providers</li> <li>• Benefits and other financial services providers</li> <li>• Professional consultants</li> <li>• Vendors necessary to complete transactions you request</li> <li>• Recipients for legal, security, or safety purposes</li> <li>• In connection with a corporate transaction</li> <li>• Business partners</li> <li>• Entities to which you have consented to the disclosure</li> </ul>
<p><b>Commercial information</b></p> <p>(Section 2.D)</p>	<ul style="list-style-type: none"> <li>• Affiliates and subsidiaries</li> <li>• Service providers</li> <li>• Benefits and other financial services providers</li> <li>• Professional consultants</li> <li>• Vendors necessary to complete transactions you request</li> <li>• Recipients for legal, security, or safety purposes</li> <li>• In connection with a corporate transaction</li> <li>• Business partners</li> <li>• Entities to which you have consented to the disclosure</li> </ul>
<p><b>Biometric information</b></p> <p>(Section 2.E)</p>	<ul style="list-style-type: none"> <li>• Fingerprint</li> <li>• Face recordings</li> <li>• Voice recordings</li> </ul>
<p><b>Internet or other electronic network activity information</b></p> <p>(Section 2.F)</p>	<ul style="list-style-type: none"> <li>• Affiliates and subsidiaries</li> <li>• Service providers</li> <li>• Professional consultants</li> <li>• Recipients for legal, security, or safety purposes</li> <li>• In connection with a corporate transaction</li> </ul>
<p><b>Geolocation data</b></p> <p>(Section 2.G)</p>	<ul style="list-style-type: none"> <li>• Affiliates and subsidiaries</li> <li>• Service providers</li> <li>• Professional consultants</li> <li>• Recipients for legal, security, or safety purposes</li> <li>• In connection with a corporate transaction</li> <li>• Entities to which you have consented to the disclosure</li> </ul>

<p><b>Audio, electronic, visual, thermal, olfactory, or similar information</b> (Section 2.H)</p>	<ul style="list-style-type: none"> <li>• Affiliates and subsidiaries</li> <li>• Service providers</li> <li>• Professional consultants</li> <li>• Recipients for legal, security, or safety purposes</li> <li>• In connection with a corporate transaction</li> <li>• Entities to which you have consented to the disclosure</li> </ul>
<p><b>Professional or employment-related information</b> (Section 2.I)</p>	<ul style="list-style-type: none"> <li>• Affiliates and subsidiaries</li> <li>• Service providers</li> <li>• Benefits and other financial services providers</li> <li>• Professional consultants</li> <li>• Vendors necessary to complete transactions you request</li> <li>• Recipients for legal, security, or safety purposes</li> <li>• In connection with a corporate transaction</li> <li>• Entities to which you have consented to the disclosure</li> </ul>
<p><b>Education information</b> (Section 2.J)</p>	<ul style="list-style-type: none"> <li>• Affiliates and subsidiaries</li> <li>• Service providers</li> <li>• Professional consultants</li> <li>• Recipients for legal, security, or safety purposes</li> <li>• In connection with a corporate transaction</li> <li>• Entities to which you have consented to the disclosure</li> </ul>
<p><b>Inferences</b> (Section 2.K)</p>	<ul style="list-style-type: none"> <li>• Affiliates and subsidiaries</li> <li>• Service providers</li> <li>• Benefits and other financial services providers</li> <li>• Professional consultants</li> <li>• Vendors necessary to complete transactions you request</li> <li>• Recipients for legal, security, or safety purposes</li> <li>• In connection with a corporate transaction</li> <li>• Entities to which you have consented to the disclosure</li> </ul>
<p><b>Sensitive personal information</b> (Section 2.L)</p>	<ul style="list-style-type: none"> <li>• Affiliates and subsidiaries</li> <li>• Service providers</li> <li>• Professional consultants</li> <li>• Recipients for legal, security, or safety purposes</li> <li>• In connection with a corporate transaction</li> <li>• Entities to which you have consented to the disclosure</li> </ul>



## 6. **Rights Concerning Personal Data**

California residents may have certain rights, subject to legal limitations, concerning the collection, use, and disclosure of Personal Data.

- **Right to Know.** You have the right to request information about the categories of Personal Data we have collected about you, the categories of sources from which we collected the Personal Data, the purposes for collecting, selling, or sharing the Personal Data, and to whom we have disclosed Personal Data and why. You may also request the specific pieces of Personal Data we have collected about you.
- **Right to Delete.** You have the right to request that we delete Personal Data that we have collected from you.
- **Right to Correct.** You have the right to request that we correct inaccurate Personal Data that we maintain about you.

California residents may exercise the rights listed above by contacting us toll-free at 1-800-461-9330, or emailing us at [GDPR@transdigm.com](mailto:GDPR@transdigm.com). We will not discriminate against you for exercising your privacy rights.

Verification: To process requests, we will need to obtain information to locate you in our records or verify your identity depending on the nature of the request. In most cases, we will collect some or all the following data elements: first and last name, email address, and telephone number. In some cases, we may request different or additional information, including a signed declaration that you are who you say you are, and will inform you if we need such information.

Authorized Agents: Authorized agents may exercise rights on behalf of California residents by submitting a request via the channels listed in the Contact Information section of this notice and indicating that they are submitting the request as an agent. We will require the agent to demonstrate authority to act on behalf of the resident by providing signed permission from the resident. We may also require the resident to verify their own identity directly with us or to directly confirm with us that they provided the authorized agent permission to submit the request.

## 7. **Data Security and Data Retention**

We maintain reasonable security procedures and technical and organizational measures to protect your Personal Data against accidental or unlawful destruction, loss, disclosure, or use.

Your Personal Data will be retained as long as necessary to fulfill the purposes we have outlined above unless we are required to do otherwise by applicable law. This includes retaining your Personal Data to maintain our employment relationship with you; to improve our business over time; to ensure the ongoing legality, safety and security of our services and relationships; or otherwise in accordance with our internal retention procedures. Once your employment or other contractual relationship with us has terminated, we may retain your Personal Data in our systems and records to ensure adequate fulfillment of surviving provisions in terminated contracts or for other legitimate business purposes, such as to enable easier future onboarding or to demonstrate our business practices and contractual obligations. If

you would like to know more about the retention periods applicable to your circumstance, you can contact us using details provided in the Contact Information section below.

**8. Accessibility for Those with Disabilities**

Should you require any accommodation with respect to this Notice, please contact us by any of the methods listed below in the Contact Information section.

**9. Contact Information**

If you have questions regarding this Privacy Notice or how Company uses your Personal Data, please contact us at:

Email: [GDPR@transdigm.com](mailto:GDPR@transdigm.com)

Mail: 1350 Euclid Avenue, Suite 1600, Cleveland, Ohio 44115

Phone: 1 (216) 706-2960