TPI Personnel Privacy Policy

TPI Composites Holdings, LLC, and its divisions, subsidiaries, and affiliates ("TPI," "Company," "we," "us," or "our") respect the privacy of the people who work for us. This Personnel Privacy Notice ("Notice") explains what personal data we collect about job applicants, current and former employees, workers, and interns (collectively, "Personnel," "you"), why we collect it, how we use, share, and protect it, how long we keep it, and the rights available to you. This Notice supplements, and does not replace, any employment contract, collective bargaining agreement, works council agreement, or offer letter you may have with TPI.

This Notice applies globally, and is supplemented by the country annexes at the end of this document for Denmark, Germany, Mexico, Spain, the United Kingdom, and the United States. Where a country annex conflicts with the global sections below, the country annex controls for individuals working in that country.

Not Applicable to Customers or Business Partners: This Notice does not apply to TPI's business customers, their representatives, or other business partners, whose data is addressed in TPI's general Privacy Policy, available here or by contacting us as described in Section 12.

Global Notice

1. Who This Notice Covers

This Notice applies to individuals who apply for employment with TPI, and to current and former employees, workers, agency staff assigned to work at TPI, and interns, wherever they are located. Where local law defines these categories differently (e.g., "workers" under UK law, or independent contractors treated differently under Mexican labor law), the country annexes address those distinctions.

2. Personal Data We Collect

The categories of personal data below will not all apply to every individual (for example, a job applicant will not yet have payroll data, and a former employee's data is more limited than a current employee's).

Category	Examples
Identification & contact data	Name, date of birth, national ID/passport number, government ID numbers required for employment eligibility (e.g., Social Security number, National Insurance number, CPR number, DNI/NIE, CURP/RFC — see country annexes), home address, personal phone number and email address, emergency contact details.
Recruitment data	CV/resume, cover letter, interview notes and scores, references, work authorization/right-to-work documentation, background check and, where legally permitted, criminal record check results, professional licenses and certifications, veteran/disability self-identification (where voluntarily provided and legally permitted).

Employment data	Job title, department, work location, employment start/end dates, manager, employment status and history, performance reviews, disciplinary records, grievance and investigation records, training records, org-chart data.
Compensation & benefits data	Salary, bonus, equity, bank account details for payroll, tax withholding elections and tax identification numbers, benefits elections (health, retirement, insurance), dependent information for benefits enrollment, leave and absence records (vacation, sick, parental, other statutory leave).
Health & safety data	Workplace injury and incident reports, occupational health assessments, disability accommodation requests and related medical information (only to the extent necessary and legally permitted), drug/alcohol testing results where required by law or role, health data connected to leave requests (e.g., a fitness-for-duty note), psychosocial risk assessment data where locally required.
IT & systems data	Corporate email and network account activity, the content of corporate email and messaging-platform communications (e.g., Microsoft Teams) sent, received, or stored using company systems, meeting recordings and transcripts, device and system logs, badge/access-control data, file contents created or modified by the employee, Generative AI prompts and interaction logs, and, at certain facilities, biometric data used for time-and-attendance or physical access control (see country annexes, in particular the U.S. annex regarding biometric information).
Location & travel data	Business travel records, expense reports, and, where used for safety or logistics at manufacturing/field sites, location data tied to site access or vehicle use.
Ethics & compliance data	Reports made through TPI's ethics/compliance hotline or whistleblowing channel (including reports made anonymously, where permitted), and related investigation records.

3. How We Use Personal Data

We use Personnel data to:

- Recruit, assess, and onboard candidates, and administer the employment relationship (contracts, promotions, transfers, terminations);
- Process payroll, taxes, and benefits, and comply with related legal and reporting obligations;
- Manage performance, training, and workforce planning;
- Maintain workplace health and safety, including incident investigation and regulatory reporting;
- Maintain the security of our facilities, systems, and data, including through access control and IT monitoring described in Section 9;

- Comply with legal, regulatory, and collective bargaining obligations, including responding to government, tax, social security, and labor authority requests;
- Operate our ethics and compliance program, including investigating reports made through our hotline; and
- Establish, exercise, or defend legal claims, and support any corporate transaction (merger, acquisition, financing, or reorganization).

We do not use Personnel data for automated decision-making, including profiling, that produces legal or similarly significant effects on an individual, without human involvement.

4. Legal Bases for Processing (EEA/UK Personnel)

For Personnel in Denmark, Germany, Spain, and the United Kingdom, our legal bases are summarized below; the country annexes address any local nuances (in particular, Germany's specific statutory basis for employee data under §26 BDSG).

Legal Basis	When It Applies
Performance of a contract	To perform the employment contract, or to take steps at your request before entering one (e.g., processing a job application).
Legal obligation	To comply with tax, social security, labor, health and safety, immigration, and other statutory obligations.
Legitimate interests	To manage our workforce, maintain security, prevent fraud, and establish or defend legal claims, where our interests are not overridden by your interests or rights.
Consent	Where we ask for it specifically (for example, certain voluntary diversity self-identification data, or optional benefits programs) — you may withdraw consent at any time without affecting the lawfulness of processing before withdrawal.
Vital interests / substantial public interest	In limited circumstances involving health and safety emergencies, or where required for employment, social security, or social protection law with appropriate safeguards.

5. How We Share Personal Data

We may share Personnel data with:

- Service providers who support HR, payroll, benefits, IT, and background-screening functions on our behalf, under contractual confidentiality and security obligations;
- Other TPI entities and affiliates, for global HR administration, IT systems, and management reporting;
- Government, tax, social security, immigration, health and safety, and labor authorities, as required by law;
- Benefits providers, insurers, and retirement plan administrators;
- Professional advisors (legal, audit, insurance) as needed;

- Works councils or employee representative bodies, where required by local law (see the Germany and Spain annexes); and
- A successor entity in connection with a merger, acquisition, financing, reorganization, or sale of some or all of our business.

We do not sell Personnel data, and we do not share it with third parties for their own independent marketing purposes.

6. International Transfers

TPI operates globally, and Personnel data may be transferred to, and processed in, the United States (where TPI is headquartered) and other countries in which TPI operates, including countries that have not been formally recognized as providing an equivalent level of data protection to your own. Where required, we implement appropriate safeguards for these transfers, such as the European Commission's Standard Contractual Clauses, the UK's International Data Transfer Addendum, or equivalent mechanisms. You can request more information about these safeguards using the contact details in Section 12.

7. Data Retention

We retain Personnel data for as long as necessary to administer the employment relationship, comply with legal and regulatory retention requirements (which vary by country and by data type — see country annexes for specifics such as payroll, tax, and personnel-file retention periods), and to establish, exercise, or defend legal claims. Recruitment data for unsuccessful candidates is generally retained for a limited period after the hiring decision, as described in the applicable country annex, unless you consent to a longer retention period for consideration of future opportunities.

8. Data Security

We maintain administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and security of Personnel data, and we require our service providers to do the same. No method of transmission or storage is completely secure, and we cannot guarantee absolute security.

9. Workplace Monitoring

Depending on your role and location, TPI may monitor use of corporate IT systems, including the content of corporate email and messaging-platform communications (e.g., Microsoft Teams), meeting recordings and transcripts, and internet and network activity, for security, compliance, and business-continuity purposes, and may operate access-control systems (including, at some facilities, biometric time-and-attendance systems) and video surveillance at TPI facilities for safety and security. Monitoring is carried out in a manner proportionate to these purposes and, where required by local law, only after consultation with employee representatives (see the Germany and Spain annexes) and with appropriate notice (see facility-level signage and IT-use policies). TPI's monitoring under this Section is based on use of TPI's networks, systems, and devices (“company assets”), regardless of whether the account being used is a corporate or personal account. For example, TPI may monitor activity involving personal email, personal cloud storage, or personal generative AI accounts where that activity occurs on or through a company asset (e.g., uploading a file from a personal email account on a company laptop, or using a personal AI account on a company device). TPI does not monitor personal devices that are not connected to or used to access TPI's networks or systems, and does not monitor the content of communications for purposes unrelated to security, compliance, or legal obligations.

10. Your Rights

Subject to the conditions and exceptions under applicable law, and as detailed further in the country annexes, you may have the right to:

- Access the personal data we hold about you, and obtain related information (purposes, categories, recipients, retention);
- Correct inaccurate or incomplete personal data;
- Request deletion of personal data, subject to our legal and record-keeping obligations;
- Restrict or object to certain processing, including processing based on legitimate interests;
- Receive a copy of personal data you provided to us in a portable format, where applicable; and
- Lodge a complaint with the relevant data protection or labor authority, or, where applicable, complain directly to TPI (see the United Kingdom annex).

To exercise these rights, contact us using the information in Section 12. We will not fulfill a request unless we can reasonably verify your identity. We will respond within the time required by applicable law.

11. Changes to This Notice

We may update this Notice from time to time to reflect changes in our practices or in applicable law. Where a change is material, we will provide notice as required by applicable law or your employment agreement (including, where applicable, consultation with works councils or employee representatives). The most recent revision date will be noted at the top of this Notice.

12. Contact Us

Questions about this Notice, or requests to exercise your rights, can be directed to:

- Email: compliance@tpicomposites.com
- Mail: TPI Composites Holdings, LLC, ATTN: Office of the General Counsel, 7500 N. Dobson Road, Suite 150, Scottsdale, AZ 85256

Country Annexes

Each annex below supplements, and should be read together with, the Global Notice above.

Annex A — Denmark

Legal framework	EU GDPR, the Danish Data Protection Act (Databeskyttelsesloven), and the Danish Act on Employers' Access to Information (in relation to certain background/criminal record checks), together with applicable Danish labor law (e.g., the Salaried Employees Act and collective agreements).
Supervisory authority	Datatilsynet

- **CPR numbers:** We process your Danish civil registration (CPR) number where necessary for payroll, tax, and social security reporting, and for pension and insurance administration — uses permitted under §11 of the Danish Data Protection Act because they are required by law. We do not use your CPR number for any other purpose (e.g., as a general employee identifier in internal systems) without a separate legal basis.
- **Criminal record and background checks:** Where a role requires a criminal record or "clean record" certificate (e.g., certain safety-sensitive or driving roles), we process this only to the extent permitted under §8 of the Danish Data Protection Act and applicable sector rules, and only for as long as necessary to assess suitability for the role.
- **Works council / cooperation committees:** Where TPI's Danish operations have a cooperation committee (samarbejdsudvalg) or are covered by a collective agreement, certain changes to monitoring or significant HR IT systems may require prior information or consultation. [Confirm applicable structure at TPI's Danish site(s).]
- **Complaints:** Danish Personnel may lodge a complaint with Datatilsynet in addition to contacting TPI directly.

Annex B — Germany

Legal framework	EU GDPR and the German Federal Data Protection Act (Bundesdatenschutzgesetz, "BDSG"), in particular §26 BDSG governing employee data, together with the Works Constitution Act (Betriebsverfassungsgesetz) where a works council (Betriebsrat) is in place.
Supervisory authority	The Federal Commissioner for Data Protection and Freedom of Information (BfDI), or the competent state (Land) authority for TPI's German entity, as applicable — [confirm which applies based on the entity's registered seat].

- **§26 BDSG as the primary basis:** For German employees, processing necessary to establish, perform, or terminate the employment relationship, and processing necessary to detect crime (in narrowly defined circumstances with documented suspicion), is generally carried out under §26 BDSG rather than the GDPR's general "legitimate interests" basis used in Section 4 of the Global Notice — the practical effect on Personnel is limited, but this is the more precise German legal basis and should be reflected as such in the German-language version of this Notice.

- **Works council co-determination:** Under §87 of the Works Constitution Act, the introduction or material change of technical systems capable of monitoring employee conduct or performance (e.g., new HRIS, time-and-attendance, or IT-monitoring tools) generally requires prior co-determination with the works council (Betriebsrat), typically documented in a works agreement (Betriebsvereinbarung). [Confirm whether TPI's German site(s) have an active works council and whether current HR/IT systems are covered by an existing works agreement; new systems should be cleared with the works council before rollout.]
- **Telecommunications/IT monitoring:** Monitoring of corporate email and internet use is subject to heightened restrictions in Germany, particularly if private use of corporate systems is permitted (which can trigger telecommunications-secrecy rules). Confirm TPI's German IT-use policy clearly prohibits or narrowly permits private use, consistent with the monitoring approach described in Section 9 of the Global Notice.
- **Whistleblowing:** Germany's Whistleblower Protection Act (Hinweisgeberschutzgesetz) governs TPI's ethics/compliance hotline as it applies to German Personnel, including confidentiality and non-retaliation protections for reports made through that channel.
- **Complaints:** German Personnel may lodge a complaint with the BfDI or applicable state authority in addition to contacting TPI directly.

Annex C — Spain

Legal framework	EU GDPR and Organic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights (LOPDGDD), which contains specific "digital rights" provisions applicable to the employment context (Title X), together with the Workers' Statute (Estatuto de los Trabajadores).
Supervisory authority	Agencia Española de Protección de Datos (AEPD)

- **Video surveillance and geolocation:** Articles 89 and 90 of the LOPDGDD specifically govern employer use of video surveillance and geolocation for labor-control purposes: employees must generally be informed in advance (via clearly visible signage for cameras, or an explicit notice for geolocation such as vehicle tracking), except in the narrow case of catching illicit conduct actually being committed.
- **Digital disconnection:** LOPDGDD Article 88 recognizes employees' right to digital disconnection outside working hours, to be respected in TPI's out-of-hours communication practices and reflected in internal policy (often addressed in a collective agreement or internal digital disconnection policy rather than this Notice itself).
- **Works council (comité de empresa) consultation:** Under the Workers' Statute, works councils generally have a right to be informed about, and in some cases consulted on, the implementation of workplace monitoring systems.
- **Whistleblowing:** Spain's whistleblowing law (Ley 2/2023) governs TPI's ethics/compliance hotline as it applies to Spanish Personnel, including required confidentiality and anti-retaliation protections, and (for employers of TPI's size) the obligation to maintain an internal reporting channel.
- **Complaints:** Spanish Personnel may lodge a complaint with the AEPD in addition to contacting TPI directly.

Annex D — United Kingdom

Legal framework	UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025 ("DUAA") — with most substantive changes effective February 5, 2026, and a new right to complain directly to employers effective June 19, 2026 — together with the Employment Rights Act 1996 and ICO employment practices guidance.
Supervisory authority	The Information Commissioner's Office (ICO), transitioning to the Information Commission under the DUAA (transition ongoing through 2026).

- **Right to complain directly to TPI:** Since June 19, 2026, UK Personnel have a statutory right to complain directly to TPI about how it has handled their personal data (Data Protection Act 2018, s.164A, as inserted by the DUAA), separate from their right to complain to the ICO/Information Commission. TPI must provide an accessible complaints channel, acknowledge receipt within 30 days, and respond without undue delay.
- **Right to work checks:** Immigration status and right-to-work documentation is collected and retained in line with UK Home Office guidance, generally for the duration of employment plus a defined period afterward (see retention schedule).
- **Workplace monitoring:** ICO guidance on monitoring at work expects monitoring to be proportionate, with a documented impact assessment for more intrusive monitoring (e.g., covert monitoring, or biometric access systems); confirm any such assessment is on file for UK sites using access-control or IT-monitoring tools described in Section 9 of the Global Notice.
- **Automated decision-making:** The UK's narrower restriction on automated decision-making (post-DUAA, limited to decisions based on special category data) applies to UK Personnel; TPI does not currently use automated decision-making of this kind in employment decisions.

Annex E — Mexico

Legal framework	The Federal Law on the Protection of Personal Data Held by Private Parties (Ley Federal de Protección de Datos Personales en Posesión de los Particulares, "LFPDPPP"), effective March 21, 2025, together with the Federal Labor Law (Ley Federal del Trabajo) and applicable social security (IMSS/INFONAVIT) reporting obligations.
Supervisory authority	Secretaría Anticorrupción y Buen Gobierno (Ministry of Anti-Corruption and Good Governance, "SABG"), which assumed data protection oversight functions following the dissolution of Mexico's former authority, INAI, effective May 9, 2025.

- **ARCO rights:** Mexican Personnel may exercise rights of Access, Rectification, Cancellation, and Opposition ("derechos ARCO") by contacting TPI as described in Section 12.
- **Statutory IDs:** We process your CURP (Clave Única de Registro de Población) and RFC (Registro Federal de Contribuyentes) as required for payroll, tax, and IMSS/INFONAVIT social security and housing-fund reporting.

- **Personnel file retention:** Certain personnel records (e.g., proof of the employment relationship, payroll records) must be retained for specific periods under the Federal Labor Law and Mexican tax law, generally longer than the retention default described in Section 7 of the Global Notice — the longer local requirement controls for Mexican Personnel.
- **NOM-035 psychosocial risk data:** If TPI conducts psychosocial risk assessments required under Mexican occupational health standard NOM-035, resulting data is treated as sensitive personal data requiring express consent and heightened confidentiality safeguards.
- **Sensitive data:** Biometric, health, and financial account data require your express consent under the LFPDPPP; where TPI uses biometric time-and-attendance systems at Mexican facilities, consent and a clear notice are obtained before enrollment (see also the U.S. annex regarding biometric data at U.S. facilities).

Annex F — United States

Legal framework	There is no single federal personnel privacy law; applicable requirements include Title VII, the ADA, and GINA (nondiscrimination and health/genetic information handling), the Fair Credit Reporting Act (background checks), I-9/immigration recordkeeping rules, state biometric privacy laws (e.g., Illinois BIPA), and, for California, the California Consumer Privacy Act as amended by the CPRA, which extends CCPA-style rights to employees.
Regulators	Vary by topic — e.g., EEOC (discrimination), state labor agencies, and, for California, the California Privacy Protection Agency.

- **Biometric data:** Certain TPI U.S. facilities use fingerprint, handprint, or facial-recognition systems for time-and-attendance or access control. Any such collection is governed by TPI's Biometric Information Privacy Policy, which addresses the written notice and consent obtained before enrollment and the applicable retention and destruction schedule. Associates with questions about biometric data collection should review TPI's Biometric Information Privacy Policy.
- **California employee privacy rights:** Since January 1, 2023, California employees, applicants, and contractors have rights under the CCPA/CPRA similar to those available to consumers, including the right to know, delete, correct, and limit use of sensitive personal information, subject to employment-context exceptions. California Personnel should receive a CCPA-compliant notice at collection; [confirm a California-specific employee notice at collection exists, either as part of this document or as a separate one-page notice provided at hire/application].
- **Background checks (FCRA):** Where TPI obtains a consumer report (background check) through a third-party agency for employment purposes, the Fair Credit Reporting Act requires a standalone disclosure and written authorization before the check, and specific pre-adverse/adverse action notices if the report affects an employment decision.
- **I-9 and immigration records:** Form I-9 and supporting work-authorization documents are retained separately from the general personnel file, for the period required by federal law (generally the later of three years after hire or one year after termination), and access is restricted accordingly.
- **State leave and paid-sick-time data:** Several states require specific recordkeeping and, in some cases, employee notice regarding paid sick/family leave balances and usage; state-specific leave notices are generally provided separately from this Notice through payroll/HRIS systems.

- **State data breach notification:** In the event of a security incident affecting Personnel data, TPI will provide notice as required by the data breach notification law of the affected individual's state of residence.
- **Genetic and health information (GINA, ADA):** Medical and genetic information (including information obtained through wellness programs or accommodation requests) is maintained separately from general personnel files with restricted access, consistent with GINA and ADA confidentiality requirements.