



TPI Privacy Policy

Section 1: Introduction

TPI Composites Holdings, LLC, and its divisions, subsidiaries, and affiliates ("TPI," "Company," "we," "us," or "our") respect your privacy. This Privacy Policy explains what personal data we collect through our website (the "Website") and in the course of our business, why we collect it, how we use and disclose it, and the choices and rights available to you. Not all personal data or purposes described below will apply to every individual.

TPI is a global manufacturer of wind turbine blades. We are principally a business-to-business company: most personal data we process belongs to our business customers, their representatives, and our business partners, rather than individual retail consumers. We are committed to complying with the data protection laws that apply to our business wherever we operate.

Not Applicable to Personnel: This Policy does not apply to our job applicants, current or former employees, independent contractors, or interns ("Personnel"). Personnel may request our separate Personnel Privacy Notice by contacting compliance@tpicomposites.com.

U.S. State Privacy Rights: If you are a resident of certain U.S. states, Section 9 (U.S. State Privacy Notice) describes additional rights available to you. If Section 9 conflicts with the rest of this Policy, Section 9 controls as to those rights.

EEA / UK / Switzerland Rights: If you are located in the European Economic Area, United Kingdom, or Switzerland, Section 10 describes the additional rights available to you under applicable data protection law.

Questions about this Policy or TPI's data practices can be directed to the contact information in Section 13 (Contact Us).

Section 2: Scope and Application

This Policy applies to personal data we collect through our Website and emails, and personal data we otherwise collect when: you purchase our products or services; you interact with us in person, by telephone, or otherwise off the Website; you are a distributor, supplier, vendor, or other business partner ("Business Partner"); or you are a Customer or a Customer's designated employee representative ("Representative"). We refer to these collectively as our "Services." Where a specific Service provides an additional privacy notice, that notice supplements this Policy.

We may create de-identified or aggregated data from personal data; that data is not personal data under applicable law and we may use it without the restrictions in this Policy. Our Services are offered globally. By using our Services, you acknowledge that your personal data may be collected and processed in the United States and in other countries in which TPI operates.

Section 3: Personal Data We Collect

Consistent with applicable law, when TPI collects personal data we will: give you timely, appropriate notice of our practices through this Policy; collect and process personal data only for specified, legitimate purposes and no more than is adequate and relevant for those purposes; use personal data consistently with the purpose for which it was collected or to which you later consented; and not use personal data for direct marketing without giving you the ability to opt out or, where required, obtaining your consent.

A. Data You Provide

We collect personal data you provide directly, such as when you browse or submit a request through our Website (including our Contact Us page), sign up for email alerts, use our mobile app, or otherwise interact or transact with us on behalf of your employer.

B. Data Collected Automatically

TPI and our service providers may automatically collect the following categories of information when you use our Services:

- **Device and browser information** (e.g., device type, browser type, IP address, operating system, device identifiers);
- **Usage information** (e.g., content viewed, features used, links clicked, and dates/times of interaction);
- **Approximate location** derived from your IP address or postal code (TPI does not collect precise, device-level geolocation); and
- **Web server logs** that record technical details of your visit.

We and our service providers collect this information using cookies, web server logs, and similar tracking technologies. Cookies are small text files stored on your device; session cookies expire when you close your browser, while persistent cookies remain to help us recognize repeat visits. You can manage cookies through your browser settings, though disabling them may affect the functionality of our Services. See Section 5 for more on your tracking choices.

Where you consent, we may combine information collected via tracking technologies with other information we hold about you, including offline data from third parties, and will treat the combined data as personal data under this Policy.

C. Data We Collect From Other Sources

We regularly receive personal data about individuals from third parties rather than directly from those individuals. This most commonly occurs when a Business Partner (such as a current or prospective customer, supplier, or channel partner) introduces one of its own Representatives to TPI as the point of contact for our business relationship, or when a colleague of a Representative provides us with that Representative's contact details in the course of a transaction.

Categories of data we receive: name, job title, business contact details (business email address and phone number), the name of your employer or organization, and the nature of your role in your organization's relationship with TPI.

Source of this data: this data typically comes directly from the Business Partner or client organization that engaged us, provided in the ordinary course of establishing or managing that business relationship (a non-public source). We may supplement this with information from publicly accessible sources, such as your employer's website or a publicly viewable professional networking profile (e.g., LinkedIn), to verify or update your business contact details.

We use this data for the same purposes described in Section 3 (How We Use Your Personal Data) — principally to establish, manage, and communicate with you about our relationship with the Business Partner or client organization you represent. We process this data on the legal bases described in Section 10.A (Our Legal Basis for Processing): principally to take steps to enter into, or to perform, a contract with your organization, and our legitimate interest in establishing and maintaining our business relationships. Where we rely on legitimate interests, that interest is maintaining and developing TPI's relationships with the representatives of our Business Partners and clients.

We may share this data with the categories of recipients described in Section 4 (How We Disclose Your Information), and we retain it as described in Section 7 (Data Retention).

When we provide this notice: where we obtain your personal data from a source other than you directly, we provide this notice within a reasonable period after obtaining the data, and in any event no later than one month after we first obtain it — or, if earlier, at the time of our first communication with you, or before we disclose your data to any other recipient.

We apply this Policy to any combined data unless we tell you otherwise.

If you are located in the EEA or UK, you have the rights described in Section 10.D (Your Rights) with respect to this data, including the right to know more about the specific source of your data in a particular case.

Section 4: How We Use Your Personal Data

We use personal data collected through our Services to: interact with you and respond to your requests; provide, maintain, and improve our Services and customer support; process transactions; communicate with you, including during contract negotiations and post-contract support, and to send you information about products and services that may interest your company; and for other business purposes consistent with this Policy and applicable law.

Section 5: How We Disclose Your Information

We do not sell or share your personal data for cross-context behavioral advertising, and we do not use it for any purpose inconsistent with this Policy or with any other statement we make to you at the point of collection. We may disclose personal data to:

- **Service providers** who perform functions on our behalf, such as IT hosting, payment processing, and customer support;

- Government authorities or other third parties where we reasonably believe disclosure is required by law, legal process, or necessary to protect TPI, our Customers, or others; and
- A successor entity in connection with a merger, acquisition, financing, reorganization, or sale of some or all of our business.

Section 6: Your Tracking Choices

Most browsers let you block or delete cookies through your browser settings; browser tools are not always effective against all tracking technologies, and blocking some cookies may affect how the Services function. Like many companies, we currently do not alter our practices in response to browser “Do Not Track” signals. Where required, we honor opt-out preference signals (such as the Global Privacy Control) as described in Section 9 (U.S. State Privacy Notice).

Section 7: Data Security

TPI maintains reasonable administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and security of personal data. No method of transmission or storage over the internet is completely secure, and we cannot guarantee absolute security.

Section 8: Data Retention

We retain personal data for as long as reasonably necessary to fulfill the purpose for which it was collected, to protect our legal rights, or as required by applicable law. Factors we consider include applicable legal or contractual retention requirements, the existence of actual or potential litigation or regulatory inquiries, the date of our last interaction with you, and the sensitivity of the data.

Section 9: Children's Privacy

Our Services are intended for individuals who have reached the age of majority in their jurisdiction of residence and are not directed to children. We do not knowingly collect personal data from children. If you believe we have inadvertently collected a child's personal data, please contact us using the information in Section 13 and we will take steps to delete it as required by law.

Section 10: U.S. State Privacy Notice

This Notice supplements the rest of this Policy and applies to "Consumers" as defined under the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and under other applicable U.S. state privacy laws (collectively, "U.S. Privacy Laws"). Capitalized terms not defined here have the meaning given in U.S. Privacy Laws. This Notice covers the twelve (12) months before the Effective Date and is updated at least annually. It does not apply to our current or former Personnel or job applicants, who may request our Personnel Privacy Notice as described on the first page of this Policy.

A. Personal Information We Collect, and Why

We collect the categories of personal information (“PI”) below directly from you (e.g., through our Website or Contact Us page) and from our affiliates, service providers, and other businesses. We use PI to provide our Services and operate our business, including to perform services, manage Customer relationships and transactions, maintain security, ensure quality, and for research and development.

TPI does not sell or share PI as those terms are defined under U.S. Privacy Laws (for example, for cross-context behavioral advertising), and does not offer any financial incentive program in exchange for PI. TPI does not currently use PI for automated decision-making or profiling that produces legal or similarly significant effects.

Category of PI	Examples
Identifiers	Name, alias, postal address, email address, IP address, online identifier, account name.
Personal records	Signature, telephone number, and financial information (e.g., payment card information).
Commercial information	Records of products or services purchased, obtained, or considered.
Internet/network activity	Browsing and interaction data on our Website, collected via cookies and similar technologies (see Sections 2.B and 5).
Approximate geolocation	Location derived from IP address or postal code.
Inferences	Inferences drawn from the above to reflect preferences or characteristics.
Sensitive PI	Government-issued identification numbers, where voluntarily provided (e.g., in connection with a transaction).

We disclose these categories of PI, for the business purposes described above, to: our IT, cloud, and other business service providers; other members of the TPI corporate group; and other parties such as government entities or litigants where required. We do not disclose any category of PI in exchange for money or other valuable consideration, and we do not disclose PI to third parties for their own independent use.

B. Your Rights

Subject to certain exemptions, you have the right to:

- **Know/Access:** request the categories of PI we have collected about you, the sources, our purposes for collecting it, and the categories of third parties to whom we have disclosed it, or a copy of the specific pieces of PI we hold about you;
- **Delete:** request deletion of PI we have collected about you, subject to exceptions such as completing a transaction, security, legal compliance, or defending legal claims;

- **Correct:** request correction of inaccurate PI we maintain about you;
- **Limit use of sensitive PI:** we only process sensitive PI for purposes that are exempt from consumer choice under U.S. Privacy Laws (e.g., to complete a transaction you requested or to comply with law);
- **Opt Out of Targeted Advertising and Certain Profiling:** opt out of the processing of your PI for targeted advertising, and of profiling in furtherance of decisions that produce legal or similarly significant effects concerning you. TPI does not currently engage in targeted advertising or this type of profiling; and
- **Appeal:** if we decline to act on a request described above, ask us to reconsider by contacting us using the information in Section 13 and noting that you are submitting an appeal. Where required by applicable law, we will respond to your appeal within the time required, and if we deny your appeal, we will provide information on how to submit a complaint to the Attorney General of your state of residence.

You may exercise these rights by contacting us using the information in Section 13 (Contact Us). We will not fulfill a request unless we can reasonably verify your identity, which may require you to provide additional information; you may also designate an authorized agent to submit a request on your behalf, subject to our ability to verify the agent's authority. We will respond within the time required by applicable law and will not charge a fee unless your request is excessive, repetitive, or manifestly unfounded.

Nevada residents have a separate right, under Nevada law, to opt out of the sale of certain covered information for monetary consideration; TPI does not sell covered information as defined under Nevada law, and Nevada residents may still submit a request to that effect using the contact information in Section 13. Where we recognize an opt-out preference signal (such as the Global Privacy Control) as described in Section 5, we do so for opt-out rights generally available under U.S. Privacy Laws, not only for California residents.

C. Non-Discrimination

We will not discriminate or retaliate against you for exercising your rights under U.S. Privacy Laws.

D. California "Shine the Light" Law

TPI does not share "personal information," as defined by California's "Shine the Light" law, with third parties for those third parties' own direct marketing purposes.

Section 11: Residents of the European Economic Area ("EEA"), United Kingdom ("UK"), or Switzerland

A. Our Legal Basis for Processing

The legal basis for our processing depends on the purpose. In summary:

Legal Basis	When It Applies
-------------	-----------------

Performance of a contract	To fulfill our obligations to Customers, or to take steps requested before entering a contract.
Legitimate interests	To operate, secure, and improve our Services and Customer relationships, to communicate about our products and services, to detect and prevent fraud or misuse, and to establish or defend legal claims — in each case, only where our interests are not overridden by your interests or rights.
Legal obligation	To comply with a legal or regulatory requirement, court order, or other legal process, including record-retention obligations.
Consent	Where we ask for it (for example, before collecting precise device location, if applicable), you may withdraw consent at any time.

TPI does not currently use your personal data for automated decision-making, including profiling, that produces legal effects concerning you or similarly significantly affects you.

B. Whether You Are Required to Provide Your Personal Data

Where you are a Representative of a Customer, providing certain personal data (such as your name and business contact details) is typically necessary for us to enter into or perform a contract with your employer; if that data is not provided, we, or your employer, may be unable to proceed with the relevant transaction or engagement. Where we ask for personal data on a voluntary basis, we will indicate this at the point of collection.

C. International Transfers

TPI operates globally, and personal data may be transferred outside the EEA, UK, or Switzerland to jurisdictions that have not been formally recognized as providing an equivalent level of data protection, including to the United States and other countries in which TPI operates, such as Mexico, China, and India. Where personal data is transferred internationally, we implement appropriate safeguards to protect that data in accordance with applicable data protection laws. Depending on the origin and destination of the transfer, these safeguards may include the European Commission's Standard Contractual Clauses, the UK's International Data Transfer Addendum, an applicable adequacy decision, Binding Corporate Rules, participation in a recognized cross-border data transfer framework (such as the EU-U.S. Data Privacy Framework), or other mechanisms recognized under applicable law as providing an adequate level of protection. Further details about the specific safeguards used for a given transfer are available upon request. For UK transfers specifically, this assessment reflects the UK's "data protection test" (whether the protection would not be materially lower than under the UK regime), which replaced the prior "adequacy-style" standard as of February 2026.

D. Your Rights

Subject to certain exceptions, you have the right to:

- **Access:** confirm whether we process your personal data and, if so, obtain a copy along with related information (e.g., purposes, categories, recipients, retention);

- **Rectification:** have inaccurate personal data corrected, or incomplete data completed;
- **Erasure:** have your personal data deleted, in circumstances such as where it is no longer necessary for the purpose collected or you withdraw consent;
- **Restriction:** limit our processing of your personal data in certain circumstances, such as while we verify its accuracy;
- **Objection:** object to processing based on our legitimate interests, unless we have compelling grounds to continue or need the data to establish or defend a legal claim;
- **Object to Direct Marketing:** object at any time, free of charge and without needing to give a reason, to our processing of your personal data for direct marketing purposes, including any related profiling; once you object, we will stop using your data for that purpose;
- **Portability:** receive personal data you provided to us, where processing is based on consent or contract and carried out by automated means, in a structured, machine-readable format;
- **Complaint:** lodge a complaint with the data protection supervisory authority in your country of residence; and
- **Complain to TPI Directly (UK only):** if you are located in the UK, complain directly to us about how we have handled your personal data, using the contact information in Section 13. We will acknowledge your complaint within 30 days and respond without undue delay, in addition to your right to complain to the UK regulator described above.

You can exercise these rights using the contact information in Section 13. We will respond within one month, extendable by a further two months for complex requests (we will let you know if an extension is needed).

E. Data Protection Officer

TPI has not appointed a statutory Data Protection Officer because, based on our current processing activities, we do not carry out large-scale systematic monitoring of individuals or large-scale processing of special categories of personal data, and are not otherwise required to do so under Article 37 GDPR or the UK GDPR. Questions about our data protection practices can be directed to the contact in Section 13 (Contact Us).

F. EU and UK Representatives

TPI has an establishment in the European Union (Spain), and is therefore not required to appoint a separate EU representative under Article 27 GDPR; TPI's EU obligations are administered through that Spanish establishment, which can be reached using the contact information in Section 13.

Section 12: Other Jurisdictions

TPI has manufacturing, sales, and administrative operations in numerous countries in addition to those specifically addressed above, including Mexico, China, and India. Where you are located in a jurisdiction not specifically addressed in Sections 9 or 10, TPI will process your personal data in accordance with this Policy and the data protection laws applicable in that jurisdiction, which may include Mexico's Federal Law on the Protection of Personal Data Held by Private Parties (as reformed effective March 21, 2025, with oversight now held by the Secretaría Anticorrupción y Buen Gobierno following the dissolution of Mexico's former data protection authority, INAI), and India's Digital Personal Data Protection Act, 2023, as applicable. You may exercise any rights available to you under such laws by contacting us as described in Section 13.

Section 13: Changes to This Policy

We may update this Policy from time to time. Changes take effect when the revised Policy is posted, and we will note the date of the most recent revision at the top of this Policy. If a change is material, we will provide additional notice as required by applicable law. Any change will apply prospectively to personal data collected after the updated Policy is posted.

Section 14: Contact Us

If you have questions about this Policy or TPI's data practices, or would like to exercise any of the rights described above, please contact us at:

Email: compliance@tpicomposites.com

Phone: (480) 305-8910

Mail: TPI Composites Holdings, LLC, ATTN: Office of the General Counsel, 7500 N. Dobson Road, Suite 150, Scottsdale, AZ 85256

Section 15: Country-Specific and Additional U.S. Addenda

The addenda below supplement Sections 9–11 above and address jurisdictions and topics with local requirements not fully captured by the general language earlier in this Policy.

Appendix A — Germany

Legal framework — EU GDPR, as implemented by the German Federal Data Protection Act (Bundesdatenschutzgesetz, “BDSG”).

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].

- **Video surveillance:** CCTV at German facilities requires specific visible-signage notices under BDSG §4, addressed at the facility level rather than in this Policy.
- **Complaints:** German residents may lodge a complaint with the BfDI or the applicable state authority, in addition to contacting TPI as described in Section 13.

Appendix B — Spain

Legal framework — EU GDPR, as implemented by Organic Law 3/2018 (LOPDGDD).

Supervisory authority — Agencia Española de Protección de Datos (AEPD).

- **Video surveillance and geolocation:** LOPDGDD Articles 89–90 require advance notice (visible signage for cameras, explicit notice for geolocation such as vehicle tracking) except in narrow circumstances.
- **Cookies:** The AEPD requires an accept/reject cookie mechanism with equal visual prominence for non-essential cookies.
- **Complaints:** Spanish residents may lodge a complaint with the AEPD, in addition to contacting TPI as described in Section 13.

Appendix C — Denmark

Legal framework — EU GDPR, as implemented by the Danish Data Protection Act (Databeskyttelsesloven).

Supervisory authority — Datatilsynet.

- **CPR numbers:** We process Danish civil registration (CPR) numbers only where permitted under §11 of the Danish Data Protection Act (e.g., a clear legal obligation or explicit consent), and do not publish them without express authority.
- **Complaints:** Danish residents may lodge a complaint with Datatilsynet, in addition to contacting TPI as described in Section 13.

Appendix D — United Kingdom

Legal framework — UK GDPR and the Data Protection Act 2018, as amended by the Data (Use and Access) Act 2025 (“DUAA”), commenced in stages from February 5, 2026 and June 19, 2026.

Supervisory authority — The Information Commissioner's Office (ICO), transitioning to the Information Commission under the DUAA.

- **Recognised legitimate interests:** The DUAA introduced a UK-only lawful basis removing the balancing test for specified purposes (e.g., crime prevention, safeguarding). This basis does not exist under EU GDPR and is distinct from the legitimate-interests basis in Section 10.A.
- **Automated decision-making:** The UK's version of Article 22 has been narrowed to restrict automated decision-making only where based on special category data, a more permissive standard than under EU GDPR.
- **International transfers:** UK outbound transfers are assessed against a “data protection

test” (not materially lower protection) rather than the prior “essentially equivalent” standard, as reflected in Section 10.C.

- **Right to complain to TPI directly:** See Section 10.D, which reflects the DUAA right in force since June 19, 2026.

Appendix E — Mexico

Legal framework — The Federal Law on the Protection of Personal Data Held by Private Parties (LFPDPPP), effective March 21, 2025, replacing the 2010 statute.

Supervisory authority — Secretaría Anticorrupción y Buen Gobierno (“SABG”), which assumed data protection oversight following the dissolution of Mexico's former authority, INAI, effective May 9, 2025.

- **ARCO rights:** Mexican residents may exercise rights of Access, Rectification, Cancellation, and Opposition (“derechos ARCO”) by contacting TPI as described in Section 13.
- **Sensitive data:** Biometric, health, and financial account data require express consent under the LFPDPPP.
- **Cross-border transfers:** Where TPI transfers Mexican personal data outside Mexico, the receiving party is expected to assume equivalent data-protection obligations to TPI.

Appendix F — Additional U.S. State-Specific Notices

This appendix supplements Section 9 with points not uniformly addressed by the general U.S. Privacy Laws framework used there.

- **Universal opt-out mechanisms:** Where we recognize browser-based opt-out signals such as the Global Privacy Control, we do so for opt-out rights generally available under U.S. Privacy Laws, consistent with Colorado and Connecticut's recognition requirements (see Section 9.B).
- **Sensitive data opt-in:** Certain state laws require opt-in consent, not merely a limitation right, before processing sensitive data such as precise geolocation, biometric or genetic data, and health data; TPI does not collect precise geolocation (Section 2.B) and does not process other sensitive-data categories without consent.
- **Illinois biometric data (BIPA):** If any TPI U.S. facility uses biometric time-and-attendance or access-control systems for individuals other than Personnel, written notice and (in Illinois) consent are obtained before enrollment, together with a published retention and destruction schedule.
- **Data broker registration:** TPI does not meet the “data broker” definition under California, Vermont, or other state laws requiring registration.

