MPM CONSORTIUM PRIVACY POLICY

Description

Document Identifier: `MPM-POL-2026-001`

Effective Date: October 5, 2026

Version: 1.0

Status: Approved by Board of Directors

1. Scope and Applicability

default watermark

This Privacy Policy governs the collection, processing, storage, and disclosure of personal data and technical credentials by the Mechanical Power Module (MPM) Consortium (â??Consortium,â?• â??we,â?• â??us,â?• or â??ourâ?•). This policy applies to:

- Authorized representatives and individual participants from **Member Organizations** (Executive, Associate, Advisory, and Academic tiers).
- Individual contributors to **Technical Working Groups (TWGs)**, the **Technical Steering Committee (TSC)**, and the **Compliance & Certification Board (CCB)**.
- Key personnel at **Accredited Testing Labs (ATLs)**.
- Applicants for **MPM Certification** (Class I, Class II, and Class III designations).
- Users accessing the **MPM Consortium Member Portal**, compliance databases, specification repositories, and public web domains.

2. Information Collected

The Consortium collects information necessary to maintain transparent industry standards, administer intellectual property policies, and operate global certification registries.

2.1 Personal Identification Information (PII)

- **Contact Details:** Full name, corporate email address, business address, telephone number, and title.
- **Organizational Affiliation:** Corporate entity, employment status, authorized voting delegate status, and team roles.
- **Authentication Data:** Usernames, hashed passwords, two-factor authentication tokens, and access logs for the MPM Member Portal.

2.2 Working Group and Standards Development Data

- **Technical Contributions:** Submitted technical specifications, code repositories, CAD schematics, meeting minutes, and audio/video recordings of TWG sessions.
- **IP Disclosures:** Essential Patent Disclosures, Royalty-Free/FRAND licensing commitments, and attribution records.
- **Voting & Ballot Records:** Formal ballots cast on specification drafts, standard ratifications, and governance amendments.

2.3 Compliance and Certification Data

- **Testing & Certification Logs:** Submitter names, lab technician signatures, telemetry logs, and compliance verification test reports generated by Accredited Testing Labs.
- **Registry Data:** Contact information for designated compliance officers supervising certified Class I (Modules), Class II (Aggregators), and Class III (Single-Use) equipment.

2.4 Digital & Telemetry Usage Data

- **Automated Data Collection:** IP addresses, browser types, session durations, access timestamps, and resource downloads across Consortium portals.

default watermark

3. Legal Basis and Purpose of Processing

The MPM Consortium processes personal data under the following legal bases and operational purposes:

Data Category	Legal Basis	Operational Purpose
Member Representation	Contractual Necessity	Administering membership agreements, billing, voting entitlements, and governance notices.
TWG Contributions & IP	Legitimate Interest & Legal Obligation	Maintaining immutable records of standard origins, licensing commitments, and contributor attributions.
Certification & Compliance	Legitimate Interest & Contractual Obligation	Verifying test authenticity, publishing valid certification seals, and enforcing non-compliance sanctions.
Portal Access & Security	Legitimate Interest	Protecting Consortium IT infrastructure, intellectual property, and restricted TWG pre-release drafts.

4. Disclosure and Information Sharing

Because the MPM Consortium is an open standards organization, certain technical contributions and certification records are publicly disclosable by design.

4.1 Public Registries and Archives

- **Public Certification Registry:** Certified equipment, vendor names, certification classes, test summary dates, and primary technical contacts are publicly accessible to verify hardware interoperability.
- **Standardization Repositories:** Contributor names, corporate affiliations, and licensing disclosures linked to ratified MPM standards are permanently archived and publicly accessible.

4.2 Internal Consortium Operations

- Personal data and voting records are shared internally among the **Board of Directors**, **TSC**, and designated administrative personnel to fulfill governance requirements.

4.3 Third-Party Processors and Service Providers

We share data with trusted third-party providers who operate under strict confidentiality agreements, including:

- Accredited Testing Labs (ATLs) conducting compliance verification.
- Cloud infrastructure, repository hosting, and identity management providers.
- Legal counsel and auditors managing IP compliance and financial audits.

default watermark

5. International Data Transfers

The MPM Consortium operates globally. Personal data and technical submissions may be transferred to, processed, and stored on servers located outside your jurisdiction, including in regions where data protection laws may differ.

For data transfers originating from the European Economic Area (EEA), the United Kingdom, or Switzerland:

- We implement Standard Contractual Clauses (SCCs) approved by the European Commission.
- We enforce organization-wide technical and administrative safeguards, including end-to-end encryption for stored compliance telemetry and portal databases.

6. Data Retention and Security

6.1 Retention Horizons

- **Governance & Standards Records:** Technical contributions, IP disclosures, TWG meeting logs, and voting history are retained **permanently** to maintain the historical and legal integrity of published MPM standards.
- **Membership & Contact Data:** Retained for the duration of active membership plus **seven (7) years** for audit and accounting compliance.
- **Security & Access Logs:** Retained for **twelve (12) months**, after which they are automatically purged or anonymized.

6.2 Security Safeguards

The Consortium employs multi-layered technical measures:

- Encryption in transit (TLS 1.3) and at rest (AES-256) across all web portals and repositories.
- Role-Based Access Control (RBAC) restricting unratified draft access to authorized TWG members.
- Regular third-party security audits and vulnerability assessments.

7. Data Subject Rights

Depending on your jurisdiction (e.g., GDPR, CCPA/CPRA), you possess specific rights regarding your personal data:

- **Right to Access & Rectification:** Request copies of your PII or update inaccurate contact information via the Member Portal.
- **Right to Erasure (Right to be Forgotten):** Request deletion of non-essential personal data. *(Note: Contributions to standards, public IP disclosures, and ratified compliance logs cannot be erased due to overriding legal and historical standard integrity requirements.)*
- **Right to Restrict or Object:** Limit processing of marketing communications or administrative notices.

default watermark

To exercise your rights, contact the Data Protection Officer at `privacy@mpmconsortium.org`.

8. Updates and Contact Information

The MPM Consortium reserves the right to amend this Privacy Policy to reflect changing regulatory requirements or governance updates. Substantive changes will be communicated via member notification **thirty (30) days** prior to taking effect.

MPM Consortium Data Protection Officer

Email: `privacy@mpmconsortium.org`

Governance Board Contact: `compliance@mpmconsortium.org`

Date Created
October 5, 2026
Author
admin