

Privacy Policy

Exported: 2026-10-15 · Source: <https://mifp.eu>

Privacy Policy — MIFP

Mediterranean Institute of Fundamental Physics

Last updated: September 2026

1. Data Controller

The Mediterranean Institute of Fundamental Physics (MIFP), with registered office at **Via Appia Nuova 31, 00047 Marino (Roma), Italy**, is the data controller for the personal data processed through this website. MIFP handles personal data in accordance with the General Data Protection Regulation (GDPR) and applicable Italian data protection law (Legislative Decree 196/2003 as amended by Legislative Decree 101/2018).

For any question about this policy or about the processing of your personal data:

- **General inquiries:** secretary@mifp.eu
- **Privacy inquiries:** secretary@mifp.eu

2. Where the Data Comes From

This website holds personal data from three different sources, and they are not interchangeable.

Data you provide directly. The only public form on this website that collects personal data is the membership application form at `/join`. It records your first and last name and e-mail address, plus any affiliation, country, field of study, position and free-text motivation you choose to provide. If e-mail delivery is enabled, the same application details are sent to MIFP's configured administrative mailbox so that the request can be reviewed. The platform also stores the username and password hash of the MIFP administrator account.

Historical and imported institutional data. MIFP's catalogue of past events, conferences and schools is built from MIFP's own historical archives and from previous MIFP websites. Imported records may therefore contain the names, affiliations and roles of people who took part in past MIFP activities, together with related programme and publication metadata. This data was not collected through this website and was not supplied by the individuals concerned through it.

Publicly available professional and scientific information. Some records are assembled from publicly available professional and scientific sources, such as published conference programmes, proceedings and institutional pages.

Imports also keep a provenance record of what was read and when, including the raw payload received from the source. That record is what makes the archive verifiable and reproducible, and it can contain the same personal data as the canonical record. It is retained for archive integrity and is covered by the retention discussion in §7.

Apart from the membership application, this website has no general enquiry form and no sign-up for events.

3. Technical Data and Aggregate Statistics

The platform does not use analytics or profiling cookies, persistent visitor identifiers, localStorage analytics, browser fingerprinting, tracking pixels or third-party tracking services. Public website statistics are produced only as server-side aggregate daily counters, without IP addresses, IP hashes, User-Agent hashes, full referrers, query strings or reconstruction of individual navigation paths.

Separate technical security and access logs exist to protect and operate the service. They may contain:

- the request path, method, status code, response size and duration;
- a **pseudonymous** client fingerprint derived from the IP address with a server-side salt, used for rate limiting and abuse detection;
- for authenticated actions, the administrator username and the action performed.

A pseudonymous identifier is not an anonymous one: it still relates to a single client and can be linked across requests. The logs are used for security and operations only, never for profiling or analytics.

Two further points of detail:

- Storing the **raw** IP address of a membership application is **disabled by default** (JOIN_STORE_RAW_IP). IP addresses are still processed transiently for rate limiting and abuse prevention.
- Logging the raw client IP into the log streams is also off by default (LOG_INCLUDE_CLIENT_IP); the salted fingerprint is used instead.

4. Special-Category Data

MIFP does not ask for special-category personal data (health, biometric data, political opinions, religious beliefs, trade-union membership, sexual orientation, genetic data) and does not need it in order to consider a membership application.

Because the motivation field of the application form is free text, please **do not include** special-category information there unless it is genuinely necessary for your request. If you do include it, it will be processed as part of your application only.

5. Purposes of Processing

Personal data is processed for these purposes only:

- reviewing and administering membership applications and the member register;
- maintaining MIFP's institutional record of past events, conferences, schools and publications;
- operating and securing the website, including administrator authentication, rate limiting and abuse prevention;
- complying with legal, tax and accounting obligations.

6. Legal Basis

Processing	Basis
Reviewing a membership application and administering the resulting membership relationship	Steps taken at the applicant's request before entering into a membership relationship, and performance of that relationship (Article 6(1)(b) GDPR)
Historical and imported institutional records of past MIFP activities	Legitimate interest in maintaining MIFP's institutional and scientific memory (Article 6(1)(f) GDPR)
Website security, rate limiting and technical logs	Legitimate interest in operating a secure service (Article 6(1)(f) GDPR)
Legal, tax and accounting obligations	Legal obligation (Article 6(1)(c) GDPR)

The membership form does not request consent for an unrelated or optional purpose: submitting it asks MIFP to take the steps needed to assess the application. The platform does not rely on Article 9 GDPR and neither requests nor requires special-category data.

7. Data Retention

Data	Retention
Membership register	Duration of membership plus 2 years
Membership applications that were rejected or archived	Up to 2 years from the decision, then eligible for deletion by the maintenance cleanup
Membership applications pending or under review	Kept until a decision is recorded
Technical access/security logs	30 days by default; rotated files are removed by the maintenance cleanup
Aggregate public statistics	Daily counters retained for 730 days; they contain no personal data
Database backups	Retained for the configured backup cycle, then aged out; see §10

Retention is enforced by the **protected maintenance cleanup**, which an operator runs deliberately from the dashboard and which always creates a verified snapshot first. It is not a continuously running scheduled job, and the application never deletes membership applications on its own.

You may request deletion of your personal data at any time using the contact address in §12.

8. Your Rights Under the GDPR

- **Access** — obtain a copy of the personal data we hold about you
- **Rectification** — have inaccurate or incomplete data corrected
- **Erasure** — request deletion of your data
- **Restriction** — limit how your data is used
- **Portability** — receive your data in a structured, machine-readable format
- **Objection** — object to processing based on legitimate interest
- **Complaint** — lodge a complaint with the Italian Data Protection Authority (Garante per la protezione dei dati personali)

These rights apply subject to the conditions and exceptions in the GDPR. To exercise them, contact secretary@mifp.eu. MIFP may need to verify your identity before acting on a request and will respond within the time limits established by applicable law.

Some of the historical and imported records described in §2 may relate to people we have no direct contact details for. Because the archive is the institutional record of past MIFP activities, such records may be restricted rather than deleted where erasure would destroy the scientific record; requests will be assessed individually.

9. Recipients and Service Providers

We do not sell, rent or share personal data for marketing or advertising purposes. Personal data may be processed by:

- **Hosting provider** — the infrastructure on which this website runs;
- **E-mail/SMTP provider** — used to deliver administrator notifications for membership applications and security/operational incidents. Security alerts may contain the minimum technical information needed to investigate an event (for example the source IP address of a failed or successful administrator login); passwords, session tokens and application secrets are never included;
- **Backup/storage provider** — where an off-site backup destination is configured;
- **Public authorities** — where we are legally required to disclose information.

The current providers, the existence of data processing agreements and any transfer assessment are organisational decisions that cannot be established from this repository. They are tracked in `docs/PRIVACY_DECISIONS_REQUIRED.md`. Where personal data is transferred outside the EEA, an appropriate Chapter V safeguard will be put in place before the processing starts.

10. Backups

Operational deletion removes data from the live database, but a copy may remain in an integrity-protected backup until that backup ages out of the normal retention cycle. Backups are kept for disaster recovery, are not used for any other purpose, and are not browsable as a data source. Deleting a record therefore takes effect immediately in normal use and finally once the relevant backups have expired.

11. Data Security

Technical and organisational measures include:

- HTTPS for all communications, with HSTS on the production deployment;
- server-side password hashing using **PBKDF2-HMAC-SHA256 with 600,000 iterations** (Werkzeug-compatible `pbkdf2:sha256` format), stored as a hash only, never as a password;
- CSRF protection on every state-changing form, using signed, expiring tokens bound to the requesting client;
- rate limiting and lockouts on administrator login and on the membership application form;
- strict access controls on the administrative area;
- data minimisation: the application stores only the fields the workflow actually uses;
- no third-party scripts, analytics or tracking services, and no external asset domains: stylesheets, JavaScript, fonts and icons are all served from this site.

12. Automated Decision-Making

We do not use automated decision-making or profiling based on personal data. Membership applications are reviewed by a person.

13. Cookies

This website sets **only strictly necessary cookies**: `mifp_admin_session`, created after a successful dashboard login, and `mifp_csrf`, a short-lived cookie created only on pages that render a form needing cross-site request forgery protection (currently `/join`, `/login` and the maintenance page). Ordinary public browsing sets no cookie at all.

There are no analytics, advertising, marketing, profiling or third-party cookies. The website shows a short informational notice about these strictly necessary cookies. It is not a consent request: closing it stores only the notice revision in your browser's `localStorage`, so the same revision is not shown again. The value is not sent to MIFP or used for tracking. No consent is collected because there is no optional storage or tracking to authorise. Full details, including cookie names, lifetimes and the notice preference, are in the [Cookie Policy](#).

14. Changes to This Policy

Any change to this Privacy Policy will be posted on this page, and the revision date at the top will be updated.

15. Contact and Complaints

- **Mediterranean Institute of Fundamental Physics (MIFP)**
- **Address:** Via Appia Nuova 31, 00047 Marino (Roma), Italy
- **Email (general):** secretary@mifp.eu
- **Email (privacy):** secretary@mifp.eu

You also have the right to lodge a complaint with the Italian Data Protection Authority (Garante per la protezione dei dati personali) at www.garanteprivacy.it.