



PRIMA FOUNDATION PRIVACY POLICY

1. INTRODUCTION

This Privacy Policy explains how the PRIMA Foundation, the implementation structure of the Partnership for Research and Innovation in the Mediterranean Area (hereinafter, “PRIMA”), safeguards personal data in compliance with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (hereinafter, “GDPR”).

This Privacy Policy explains how the PRIMA Foundation collects, holds and processes personal data based on the following grounds:

- Consent: processing is based on consent the interested party has given to us;
- Performance of a contract: processing is necessary for the performance of a contract;
- Compliance with our legal obligations: processing is necessary for compliance with EU rules, Spanish law and other legal obligations; and
- Legitimate interests: processing is necessary for the purposes of the legitimate interests pursued by us or by a third party, except where such interests are overridden by the interested party interests or his/her fundamental rights and freedoms.

For each category of data subject, it is explained the purpose for which PRIMA collects personal data, how PRIMA controls access to personal data, and the legal grounds for collecting, processing and holding the personal data.

2. TYPE OF PERSONAL DATA PRIMA COLLECTS, HOLDS AND PROCESSES AND LAWFUL BASIS

2.1. Category A: personal data related to job vacancies

The personal data PRIMA collects, holds and process regarding applicants to job adverts are:

- Name
- Address
- Employer
- Email address(es)
- Employment history
- Educational background
- Any other additional information the applicant may put on his/her CV

The personal data PRIMA collects, holds and processes under this category is used for shortlisting suitable candidates for vacant positions, inviting candidates for interview, and for drawing up contracts for the selected candidates.

The applications received are kept in our recruitment inbox or in the platform created to receive the submissions, which is secure, and is restricted to HR and those involved in the selection



process committee. On the day of the interview, CVs and application letters of shortlisted candidates are given to interviewers of the selection process committee for making references to during the interview. All documents printed for interviewers are shredded immediately after the interview.

By applying for a vacant position, the interested party has given PRIMA consent to hold and process his/her application.

2.2. Category B: personal data related to the attendance to events organized by PRIMA

The personal data PRIMA collects, holds and processes for individuals who are interested in attending the PRIMA Infoday event (or any other event organized by PRIMA):

- Name
- Organisation/institution the interested part work for
- Email address(es)

The personal data PRIMA collects, holds and processes under this category are used solely for sending the invitation to the PRIMA Infoday (or other PRIMA events) and is accessible only by the PRIMA staff in charge of sending the invitation the event.

By registering to the PRIMA Infoday (or other PRIMA events) the interested party has given to PRIMA consent to process and hold his/her personal data.

2.3. Category C: personal data related to PRIMA current and previous employees

The personal data PRIMA collects, holds and processes for its current and previous employees are:

- Copy of the passports or other identity documents (and family members if this is the case)
- Copy of the resident permits and visas (if required)
- Copy of diplomas and certificates
- Date of birth and remuneration details
- References and CV
- Home address
- Sick leave details
- Telephone numbers
- Country of origin
- Performance appraisal information
- BSN number
- Bank details

The personal data PRIMA collects, holds and processes under this category are used to sign the labors contracts with PRIMA, for making salary and other statutory payments; complying with statutory obligations; making visa applications (if required); assigning office equipment (mobile phone, laptops, and PCs); creating logins; making honorarium payments; flight bookings; hotel bookings; publishing the information on the website; and ensuring compliance with our internal policies and procedures.



Access to the personal data regarding personnel records is restricted to PRIMA HR responsible and the Accounting and Financial Manager. All HR related documents are kept in either secured cabinets or in one of our secure computerized systems.

PRIMA reasons for collecting, processing and holding personal data under this category include:

- Compliance with legal obligation;
- Performance of employment contract;
- Legitimate interests; and
- Consent.

The name and job title of PRIMA current employees are placed on the PRIMA website based on consent of PRIMA employees.

2.4. Category D: personal data related to applicants to PRIMA calls

The personal data PRIMA collects, holds and processes for applicants who apply on PRIMA calls are:

- Name
- Email address
- Phone number
- Employer or organisation/institution the applicant works for

The personal data PRIMA collects, holds and processes under this category are used solely for selecting those proposals that will be funded under the PRIMA calls and is accessible only by the PRIMA staff and the independent experts appointed for the evaluation proposals.

By submitting proposals to the PRIMA calls the applicants have given to PRIMA consent to process and hold his/her personal data for this purpose.

2.5. Category E: personal data related to professionals (consultants, contractors, freelancers or experts) performing work on behalf of PRIMA

The personal data PRIMA collects, holds and processes for professionals who work on behalf of the organization are:

- Name
- Address
- Employer
- Email address(es)
- Employment history and educational background (CV)
- Copy of passport
- Bank details
- Nationality

The personal data PRIMA collects, holds and processes under this category are used for recruitment of professionals, making honorarium payments and other justified expenses, and ensuring compliance with our internal policies and procedures.



Access to the personal data regarding this category is restricted to PRIMA staff, and service providers where required.

Our reasons for collecting, processing and holding personal data under this category include:

- Compliance with legal obligation;
- Performance of contract;
- Legitimate interests; and
- Consent.

Any processing of personal data related to the recruitment of professionals is based on consent.

PRIMA requests for expressions of interests from experts who are interested in becoming independent PRIMA evaluators.

Personal data received from applications is entered in PRIMA database of experts. This processing is also based on consent. By completing an application form, the applicant has given PRIMA consent to hold and process your application

2.6. Category F: personal data related for Board of Trustees, Steering Committee and Scientific Advisory Committee members

The personal data PRIMA collects, holds and processes for members of the PRIMA Foundation bodies are:

- Name
- Professional address
- Employer
- Email address(es)
- Copy of passport
- Nationality

The personal data PRIMA collects, holds and processes under this category are used for meeting communications and notifications, making payments of justified expenses, and ensuring compliance with internal policies and procedures.

Access to the personal data regarding this category is restricted PRIMA staff and service providers where required.

PRIMA reasons for collecting, processing and holding personal data under this category include:

- Compliance with legal obligation;
- Legitimate interests; and
- Consent.



3. RETENTION OF DATA

PRIMA retains personal data only for as long as is necessary to fulfill the purposes for which they were collected or processed, in compliance with the GDPR and Spanish regulations. Retention periods vary depending on the type of data subject and the nature of the data, as detailed below. Data will be securely deleted or anonymized once the retention period has expired, unless a longer retention period is required for legal obligations or the establishment, exercise, or defense of legal claims.

1. Personal data related to job vacancies:
Retained for 1 year following the conclusion of the recruitment process.
2. Personal data related to attendance at PRIMA events:
Retained for 1 to 3 years to manage event-related activities and reporting obligations.
3. Personal data related to current and previous employees:
Retained for 6 to 10 years, in line with employment, tax, and legal record-keeping requirements.
4. Personal data related to applicants for PRIMA calls:
Retained for 2 to 3 years to manage applications and related funding activities.
5. Personal data related to professionals (consultants, contractors, freelancers, or experts):
Retained for 6 to 7 years for contract management, tax, and financial purposes.
6. Personal data related to members of PRIMA Foundation bodies:
Retained for 3 to 5 years after the individual's term ends for legal, administrative, and reporting purposes.

These retention periods are subject to review and may be updated as necessary to comply with legal requirements, including the GDPR and Spanish regulations. Data will be securely deleted or anonymized once the retention period has expired, unless further retention is required for compliance with legal obligations or the establishment, exercise, or defense of legal claims.

4. TRANSFER OF PERSONAL DATA TO THIRD PARTIES AND AUDIT COMPLIANCE

PRIMA may share personal data with third parties when necessary to fulfill its operational or legal requirements, including for administrative tasks, event organization, or regulatory compliance. Specific third parties that may receive personal data include:

- Experts/evaluators: Independent experts involved in the evaluation of proposals, who will process personal data strictly for evaluation purposes.
- Auditors: PRIMA may share personal data with external auditors.
- European Commission (EC): PRIMA may need to share personal data with the EC, including the European Court of Auditors, OLAF (European Anti-Fraud Office), and EC operational auditors, for the purpose of financial and operational audits, and ensuring compliance with EU financial regulations.



- **Service Providers:** External service providers contracted by PRIMA to assist with activities such as IT services. These service providers are carefully selected and are required to comply with strict confidentiality and data protection standards.

Personal data is shared only for the purposes specified at the time of collection. PRIMA ensures that all third-party processors comply with GDPR. For added assurance, PRIMA's tender Terms of Reference require all contracted third parties to handle personal data in full compliance with GDPR.

In line with its commitment to data protection, PRIMA conducts a due diligence process based on its internal procedure when selecting third-party service providers or partners who will handle personal data. This process includes a thorough evaluation of the third party's technical and organizational measures to ensure compliance with GDPR. As part of the selection, PRIMA reviews their data protection practices, data handling capabilities, and safeguards to confirm that they meet the necessary standards. This assessment is taken into account in the procedures by which PRIMA selects third parties, and ensures that all parties contracted by PRIMA comply with the required data protection regulations.

PRIMA also employs technical and organizational safeguards to protect personal data during these transfers, and any third parties involved are contractually obligated to maintain data privacy and confidentiality.

5. RIGHTS OF THE INTERESTED PARTY AND PRIMA DATA PROTECTION OFFICER

In accordance with GDPR the interested party (individual whose data is processed) have the right to obtain access to the personal data held by PRIMA and to request its rectification or erasure, or restriction of processing or, where applicable, the right to object to processing or the right to data portability. Where the processing is based on the party consent or explicit consent, the party has also have the right to withdraw his/her consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

In particular, the interested party can:

5.1. Right of access

The right to obtain confirmation as to whether PRIMA holds personal data about them, and if so, access to that data.

5.2. Right of rectification

The right to request the correction of inaccurate or incomplete personal data held by PRIMA.

5.3. Right to erasure

The right to request the deletion of personal data when the continued processing of that data is no longer justified under applicable laws.

5.4. Right to restriction of processing



The right to request the restriction of processing their personal data, where applicable, under the conditions set out in the GDPR.

5.5. Right to object

The right to object to the processing of personal data on grounds relating to their particular situation, including for direct marketing purposes.

5.6. Right to Data Portability

The right to receive the personal data concerning them, in a structured, commonly used, and machine-readable format, and transmit this data to another controller.

5.7. Right to Withdraw Consent

The interested party has the right to withdraw their consent at any time, without affecting the lawfulness of processing that occurred before the withdrawal.

The interested party can exercise his/her rights by contacting the PRIMA Data Protection Officer, who also acts as PRIMA's Legal Officer (julia.rebes@prima-med.org).

The interested party also has the right to lodge a complaint with the supervisory authority (Agencia Española de Protección de Datos, <https://www.aepd.es/es>) regarding the use of personal data by PRIMA.

6. PROCEDURE FOR EXERCISING RIGHTS

To exercise any of the rights listed in Section 5, the interested party should follow the procedure outlined below:

6.1. Contact PRIMA's Data Protection Officer (DPO):

Name: Julià Rebés
Email: julia.rebes@prima-med.org

6.2. Specify the right being exercised:

The interested party should clearly state which right they wish to exercise (e.g., access, rectification, erasure, etc.).

6.3. Provide details of the request:

Where applicable, the interested party should specify the personal data involved in the request to help PRIMA process it efficiently.

6.4. Verification of Identity:

PRIMA may request additional information to verify the identity of the interested party before processing the request. This is done to ensure that the request is legitimate and to protect the data subject's privacy.

6.5. Response timeline:



Upon receiving a valid request, PRIMA will respond within one month. This period may be extended by up to two months for complex or multiple requests, and the interested party will be informed within one month of the extension.

6.6. Refusal of request:

If PRIMA is unable to fulfill the request, a clear explanation will be provided, including the legal basis for the refusal.

6.7. Lodging a complaint:

If the interested party believes that their rights have not been respected, they can lodge a complaint with the Agencia Española de Protección de Datos (<https://www.aepd.es/es>) or seek a judicial remedy.

7. Data breach management procedure

In the event of a data breach, PRIMA will promptly assess the nature and impact of the breach, notify the relevant authorities if necessary, and inform affected individuals without undue delay, in accordance with GDPR requirements. PRIMA follows an internal procedure for managing data breaches, which includes the following steps:

7.1. Detection and containment:

Upon identifying a breach, PRIMA will take immediate action to contain it and prevent further damage. This includes securing affected systems and minimizing unauthorized access to personal data.

7.2. Impact assessment:

The Data Protection Officer (DPO) and relevant staff will evaluate the breach's nature and scope, including the type of data involved, the number of individuals affected, and the potential consequences.

7.3. Notification to authorities:

If the breach poses a risk to individuals' rights and freedoms, PRIMA will notify the relevant supervisory authority, such as the Agencia Española de Protección de Datos, within 72 hours of becoming aware of the breach.

7.4. Notification to affected individuals:

If the breach is likely to result in a high risk to individuals, PRIMA will inform affected individuals without undue delay, explaining the breach's nature and the steps being taken to mitigate any potential harm.

7.5. Mitigation and prevention:

PRIMA will take necessary steps to mitigate any harm caused by the breach, including offering support to affected individuals and implementing additional security measures to reduce the likelihood of future incidents.



8. CONTACT INFORMATION

For any inquiries regarding the processing of personal data by PRIMA or to exercise your rights under the GDPR, the interested party may contact the PRIMA Data Protection Officer at the following contact details:

Data Protection Officer

PRIMA Foundation

Email: julia.rebes@prima-med.org

Telephone: +34 930 190 818

Postal address: Carrer Jordi Girona, 29 Nexus 2 Building, office 2A - 08034 – Barcelona (Spain)

SUMMARY CHART

Field	Details
Controller	PRIMA Foundation
Purpose of processing	The processing of personal data is required for various administrative, contractual, and legal purposes related to employment, event management, project applications, and board member communications.
Types of personal data	Category A (Job applicants):
	Name, address, email, employment history, educational background, CV details.
	Category B (Event attendees):
	Name, organization, email.
	Category C (Employees):
	ID documents, performance reports, salary details, etc.
	Category D (PRIMA calls applicants):
	Name, email, phone number, employer/organization.
Legal Basis for Processing	Category E (Consultants/Professionals):
	Name, email, CV, passport, bank details, nationality.
Legal Basis for Processing	Category F (Board/Committee members):
	Name, professional address, email, passport copy, nationality.
	- Consent (job applicants, event attendees, professionals, and board members)
	- Contractual necessity (employment contracts, PRIMA calls applicants)
Recipients of personal data	- Compliance with legal obligations (tax, labor laws)
	- Legitimate interests (project management, recruitment)
	- PRIMA HR and finance departments for employees
	- Independent experts for project proposal evaluations
	- European Commission and regulatory bodies
Retention period	- Event management staff
	- External service providers (e.g., IT, legal, event coordinators)
	- Job applicants: Retained for 6 months after the recruitment process.
	- Event attendees: Retained for up to 1 year for communication related to the event.
	- Employees: Retained for the duration of employment and up to 6 years after termination (in compliance with tax and employment laws).
	- PRIMA calls applicants: Retained for 1 year after the call submission deadline.
Data security measures	- Consultants/Professionals: Retained for the duration of the contract and up to 5 years.
	- Bodies members: Retained for the duration of membership and for statutory reporting purposes.
Data transfers	- Personal data is stored in secured systems with access controls.
	- Paper documents are kept in locked cabinets.
Data transfers	- Data may be transferred to third-party service providers (e.g., IT, auditors, and event management companies).
	- Data may be shared with the European Commission, including the European Court of Auditors, OLAF (European Anti-Fraud Office), and EC operational auditors, for compliance and auditing purposes.



PRIMA privacy policy version 2.0
November 2024
Approved by the PRIMA Secretariat Director