ORGANISATIONAL POLICY

# Data protection and digital tools policy

Responsible use of information in activities, projects and communications

| | |
|---|---|
| **Version** | 2.0 |
| **Revision** | 28 August 2026 |
| **Effective date** | 1 October 2026 |
| **Next ordinary review** | 1 October 2028 |

**OUR COMMITMENT**

Io Per l'Altro - APS uses personal data and digital tools to deliver educational, membership and project activities. The Association protects people's dignity and autonomy, collects only what is needed, and makes purposes, responsibilities, periods and rights understandable.

**GUIDING PRINCIPLE**

Data is not collected merely because it might be useful: it is collected when there is a clear purpose, an appropriate legal basis, controlled access and a deletion date.

## 1. Purpose and scope

This policy applies to processing carried out in Italy and abroad, on paper or through digital tools, in governance, volunteering, selection, Erasmus+ and other projects, events, mobility, training, communications, administration, partnerships and procurement.

- Board members, members, volunteers, employees, contractors and professionals
- applicants and participants, accompanying persons, families and emergency contacts
- partners, funders, suppliers, donors and institutional contacts
- website visitors, communication recipients and people appearing in images, video or testimonials

This policy does not replace specific privacy notices, the website and cookie notice, processor agreements, media permissions or the terms of institutional platforms.

## 2. Controller and responsibilities

| Role | Core responsibility |
|---|---|
| Data controller | Io Per l'Altro - APS, represented by President Marco Valerio Battaglia, determines the essential purposes and means of processing. |
| Board of Directors | Approves policies and resources and reviews material risks and updates. |
| President | Receives rights requests and breach reports and coordinates institutional decisions, authorities and providers. |
| Project lead | Defines necessary data, authorised persons, partner recipients and end-of-project deletion. |
| Communication & Dissemination Manager | Checks permissions and context before publishing images, video, names or testimonials. |
| Quality & Monitoring Manager | Maintains records, controls and organisational learning, without automatic access to participant special-category data. |
| Authorised persons | Access data only for assigned tasks, maintain confidentiality and immediately report anomalies. |

**NO DPO APPOINTED**

The President is the operational and institutional privacy contact, but this does not make him the formally independent Data Protection Officer (DPO). Any duty or benefit of appointing a DPO is reviewed as activities change.

## 3. Processing principles

- lawfulness, fairness and transparency towards individuals
- specified purposes and no incompatible reuse

- minimisation: requesting practical instructions rather than unnecessary health detail
- accuracy and the ability to update information
- limited retention, with deadlines and documented deletion
- integrity, confidentiality, availability and demonstrable accountability
- data protection by design and by default

## 4. Data and sources

| Category | Examples |
|---|---|
| Identity and contact | name, surname, date of birth where needed, email, phone, residence or identity document only when required by the project |
| Participation | motivation, availability, role, attendance, learning outcomes and feedback |
| Administration | contracts, payments, reimbursements, tax details and funder-required documentation |
| Health and accessibility | allergies, intolerances, medication, needs and strictly necessary practical instructions |
| Image and voice | photographs, video, audio, testimonials and attribution preferences |
| Digital use | accounts, permissions, available logs, project messages and data required by platforms |

Data normally comes from the individual, a person holding parental responsibility, a group leader or partner who has informed the individual, or programme platforms and authorities. Source and applicable notice are recorded where they are not self-evident.

## 5. Purposes and legal bases

Each specific notice identifies purpose and legal basis. The Association may process data to perform agreements and requested activities, comply with legal or funder duties, protect vital interests, pursue assessed and proportionate legitimate interests, or on the basis of freely given and withdrawable consent.

- consent is not used where processing is genuinely necessary to organise a project or comply with a duty
- health or other special-category data is processed only with a valid Article 9 GDPR condition, normally explicit consent for requested support or vital interests in an emergency
- refusing public images, video, newsletters or testimonials does not prevent participation
- Io Per l'Altro does not make solely automated decisions producing legal or similarly significant effects on individuals

## 6. Notices, choice and vulnerable people

Information is provided in clear language before collection or, where data comes from third parties, within the required period. For children and people who may face comprehension barriers, accessible explanations are used, persons holding parental responsibility are involved where required, and the individual's wishes are considered according to age and capacity.

> **REQUIRED AND OPTIONAL DATA**
> Forms clearly distinguish what is needed to participate from what is optional. Broad consent is not made a condition of access to an activity.

## 7. Photographs, video and testimonials

- a separate, preferably digital process is used, with distinct choices for website, social media, project materials and partner channels

- a person may participate without authorising publication and may request practical alternatives during group filming
- before publication, consent or another applicable basis, context, attribution, dignity and absence of unnecessary sensitive information are checked
- images of children are not requested or exchanged privately; only project-controlled channels and legally required permissions are used
- withdrawal applies to future uses; the Association removes material it controls, while third-party copies, shares and caches may not be fully recoverable
- testimonials may be anonymous, first-name only or full-name according to the person's documented choice

## 8. Digital tools and messaging

| Tool | Minimum rule |
|---|---|
| Gmail, Drive, Forms and Classroom | named accounts, project folders, limited permissions and access removal at closure |
| WhatsApp | operational communications; no identity documents or detailed health data, except the minimum necessary in an urgent situation |
| Canva and creative tools | already authorised or anonymised content; no parallel participant-data archive |
| Erasmus+ platforms | only programme-required data and information to individuals about applicable institutional privacy notices |
| Digital forms | minimum fields, linked notice, restricted access and a defined closure/deletion date |

Where reasonably possible, anyone who does not wish to join a messaging group is offered another route for essential information. Groups are not reused for unrelated purposes.

## 9. Partners, providers and transfers

Partners normally receive only name, surname, date of birth and practical allergy or intolerance information where needed. Before any sharing, role, purpose, legal basis, security, period and deletion are defined. Providers processing data for the Association are bound, where applicable, by an Article 28 GDPR agreement.

- sharing uses restricted links or agreed channels, not public folders
- for transfers outside the European Economic Area, applicable adequacy decisions or safeguards and service risks are checked
- a partner may not use data for its own campaigns or further purposes without an independent basis and its own notice

## 10. Security and access control

- personal accounts, strong passwords and multi-factor authentication where available
- need-to-know access: normally the President and project lead for participant data
- separate folders for each project and for health, incident or safeguarding information
- no automatic forwarding to unauthorised personal email and no links open to anyone
- devices protected by locking, updates and remote wipe where available
- periodic access review, revocation when the task ends and proportionate backups
- printing only where necessary, locked storage and secure destruction

## 11. Retention and deletion

Each project sets periods linked to purpose and legal, tax, insurance and funder duties. Health information, emergency contacts and document copies are deleted as soon as the operational need ends, normally at project closure. Identity-document copies are not retained without a specific documented need.

- administrative, contractual and reporting records follow applicable periods
- consents and withdrawals are retained as needed to evidence choices and manage authorised uses
- incident, complaint and safeguarding records use restricted storage and separate periods based on protection and potential claims
- closure covers Drive, Forms, Classroom, local downloads, email, devices and paper copies

## 12. Individual rights

Individuals may request access, rectification, erasure, restriction, portability where applicable, objection and withdrawal of consent without affecting prior lawfulness. They may also lodge a complaint with the Italian Data Protection Authority.

> **RESPONSE TIME**
> The request is recorded, identity is verified proportionately and a response is provided without undue delay, normally within one month. In complex cases the period may be extended under the GDPR, with the individual informed within the first month.

## 13. Personal data breaches

> **IMMEDIATE REPORTING**
> Anyone who loses a device, sends data to the wrong person, exposes a link, experiences unusual access or detects loss, alteration or unavailability immediately informs the President. Evidence is not deleted and individuals or authorities are not contacted independently.

The Association contains the event, documents facts and effects and assesses risk to individuals. Where required, it notifies the Authority without undue delay and, where feasible, within 72 hours of awareness; if risk is high, affected individuals are also informed in clear language. Every breach is recorded, including those not notified, with the rationale for the decision.

## 14. Artificial intelligence

- identifiable, health, safeguarding or participant-document data is not entered into generative tools
- anonymised, aggregated, synthetic or already-publication-ready data is used after checking service terms and settings
- AI does not decide selection, eligibility, support or disciplinary measures; every output is reviewed by a competent person
- materials, images and testimonials are not used to train systems or create imitations without a specific basis and clear information

## 15. Training, control and review

- each team receives proportionate instructions on the data it uses and permitted channels
- the processing register, providers and access rights are reviewed at least annually

- new tools, special-category data, systematic monitoring or high-risk processing require prior assessment and, where necessary, a data protection impact assessment
- the policy is reviewed every two years and after breaches, legal change, new countries, tools or activities

## 16. Contact

| | |
|---|---|
| **Controller** | Io Per l'Altro - APS |
| **Tax code** | 97786260584 |
| **Registered office** | Via Agostino Scaparro 7, 00122 Rome, Italy |
| **RUNTS** | G09433 |
| **Privacy and rights email** | ipaostia@gmail.com |
| **Certified email** | ioperlaltro@pec.it |
| **Website** | www.ioperlaltro.com |
| **Legal representative** | Marco Valerio Battaglia |

## 17. References


- Regulation (EU) 2016/679 (GDPR), particularly Articles 5, 6, 9, 12-22, 24-25, 28, 30, 32-35 and 44-49.
- Italian Legislative Decree 196/2003, as amended by Legislative Decree 101/2018.
- Italian Data Protection Authority: processing principles, records of processing and personal data breaches.
- Erasmus+ Programme Guide 2026 and privacy statements for Erasmus+ platforms.

https://eur-lex.europa.eu/eli/reg/2016/679/oj/ita
https://www.garanteprivacy.it/home/principi-fondamentali-del-trattamento
https://www.garanteprivacy.it/registro-delle-attivita-di-trattamento
https://www.garanteprivacy.it/data-breach
https://erasmus-plus.ec.europa.eu/programme-guide/part-c/other-provisions
https://erasmus-plus.ec.europa.eu/erasmus-and-your-data

# Approval

| | |
|---|---|
| **Approved by** | Board of Directors of Io Per l'Altro - APS |
| **Resolution date** | 30 Agosto 2026 |
| **Effective date** | 1 October 2026 |
| **Legal representative's signature** | Marco Valerio Battaglia |