POLICY ISTITUZIONALE

Policy per la protezione dei dati e gli strumenti digitali

Uso responsabile delle informazioni nelle attività, nei progetti e nella comunicazione

Versione	2.0
Revisione	28 agosto 2026
Entrata in vigore	1 ottobre 2026
Prossima revisione ordinaria	1 ottobre 2028
Approvazione	Consiglio direttivo - data della delibera da inserire
Classificazione	Documento pubblico

IL NOSTRO IMPEGNO

Io Per l'Altro - APS utilizza dati personali e strumenti digitali per realizzare attività educative, associative e progettuali. L'Associazione protegge la dignità e l'autonomia delle persone, raccoglie soltanto ciò che serve e rende comprensibili finalità, responsabilità, tempi e diritti.

PRINCIPIO GUIDA

Un dato non si raccoglie perché potrebbe essere utile: si raccoglie quando esistono una finalità chiara, una base giuridica adeguata, un accesso controllato e una data di cancellazione.

1. Finalità e campo di applicazione

La policy si applica ai trattamenti svolti in Italia e all'estero, su carta o con strumenti digitali, nell'ambito di governance, volontariato, selezione, progetti Erasmus+ e altri programmi, eventi, mobilità, formazione, comunicazione, amministrazione, partenariati e forniture.

- membri del Consiglio direttivo, soci, volontari, dipendenti, collaboratori e professionisti
- candidati e partecipanti, accompagnatori, famiglie e contatti di emergenza
- partner, finanziatori, fornitori, donatori e contatti istituzionali
- visitatori del sito, destinatari di comunicazioni e persone presenti in immagini, video o testimonianze

Questa policy non sostituisce le informative specifiche rese alle persone, l'informativa cookie e sito, gli accordi con i responsabili del trattamento, le liberatorie media o le condizioni delle piattaforme istituzionali.

2. Titolare e responsabilità

Ruolo	Responsabilità essenziale
Titolare del trattamento	Io Per l'Altro - APS, rappresentata dal Presidente Marco Valerio Battaglia, determina finalità e mezzi essenziali del trattamento.
Consiglio direttivo	Approva policy e risorse, valuta rischi rilevanti e revisioni.
Presidente	Riceve richieste sui diritti e segnalazioni di violazione; coordina decisioni istituzionali, autorità e fornitori.
Responsabile di progetto	Definisce i dati necessari, le persone autorizzate, i partner destinatari e la cancellazione a fine progetto.
Communication & Dissemination Manager	Verifica permessi e contesto prima di pubblicare immagini, video, nomi o testimonianze.
Quality & Monitoring Manager	Mantiene registri, controlli e apprendimento organizzativo, senza accesso automatico ai dati sensibili dei partecipanti.
Persone autorizzate	Accedono solo per il compito assegnato, rispettano riservatezza e segnalano immediatamente anomalie.

NESSUN DPO DESIGNATO

Il Presidente è il contatto operativo e istituzionale per la privacy, ma non assume per questo il ruolo formale e indipendente di Responsabile della protezione dei dati (DPO). L'eventuale obbligo o opportunità di nomina viene riesaminato al mutare delle attività.

3. Principi del trattamento

- liceità, correttezza e trasparenza verso le persone
- finalità determinate e nessun riutilizzo incompatibile

- minimizzazione: chiedere istruzioni pratiche anziché dettagli sanitari non necessari
- esattezza e possibilità di aggiornamento
- conservazione limitata, con scadenze e cancellazione documentata
- integrità, riservatezza, disponibilità e responsabilizzazione verificabile
- protezione dei dati fin dalla progettazione e per impostazione predefinita

4. Dati trattati e fonti

Categoria	Esempi
Identità e contatti	nome, cognome, data di nascita quando necessaria, email, telefono, residenza o documento solo se richiesto dal progetto
Partecipazione	motivazione, disponibilità, ruolo, presenze, risultati di apprendimento e feedback
Amministrazione	contratti, pagamenti, rimborsi, coordinate fiscali e documentazione richiesta dal finanziatore
Salute e accessibilità	allergie, intolleranze, farmaci, esigenze e istruzioni pratiche strettamente necessarie
Immagini e voce	fotografie, video, audio, testimonianze e preferenze di attribuzione
Uso digitale	account, autorizzazioni, log disponibili, messaggi di progetto e dati richiesti dalle piattaforme

I dati provengono normalmente dalla persona interessata, da chi esercita la responsabilità genitoriale, dal group leader o partner che ha informato la persona, oppure da piattaforme e autorità del programma. La provenienza e l'informativa applicabile vengono registrate quando non sono immediate.

5. Finalità e basi giuridiche

Ogni informativa specifica indica finalità e base giuridica. L'Associazione può trattare dati per eseguire accordi e attività richieste dalla persona, adempiere obblighi legali o del finanziatore, proteggere interessi vitali, perseguire interessi legittimi valutati e proporzionati, oppure sulla base di un consenso libero e revocabile.

- il consenso non viene usato quando il trattamento è realmente necessario per organizzare il progetto o adempiere un obbligo
- i dati relativi alla salute o ad altre categorie particolari sono trattati solo con una condizione valida ai sensi dell'articolo 9 GDPR, normalmente consenso esplicito per il supporto richiesto o interessi vitali in emergenza
- rifiutare immagini, video, newsletter o testimonianze pubbliche non impedisce la partecipazione
- Io Per l'Altro non adotta decisioni esclusivamente automatizzate che producano effetti giuridici o analogamente significativi sulle persone

6. Informative, scelta e persone vulnerabili

Le informazioni sono rese in linguaggio chiaro prima della raccolta o, quando i dati provengono da terzi, nei tempi previsti. Per minorenni e persone che possono incontrare ostacoli di comprensione si utilizzano spiegazioni accessibili, si coinvolge chi esercita la responsabilità genitoriale quando richiesto e si considera la volontà della persona in modo adeguato all'età e alla capacità.

> **DATI NECESSARI E DATI FACOLTATIVI**
> I moduli distinguono chiaramente ciò che serve per partecipare da ciò che è facoltativo. Non si inseriscono consensi generici come condizione per accedere a un'attività.

7. Fotografie, video e testimonianze

- si usa una procedura separata, preferibilmente digitale, con scelte distinte per sito, social, materiali del progetto e canali dei partner
- la persona può partecipare senza autorizzare la pubblicazione e può chiedere alternative pratiche durante riprese di gruppo
- prima della pubblicazione si verificano consenso o altra base applicabile, contesto, attribuzione, dignità e assenza di informazioni sensibili non necessarie
- con i minorenni non si richiedono o scambiano immagini in privato; si usano esclusivamente canali controllati dal progetto e le autorizzazioni legalmente necessarie
- la revoca vale per gli usi futuri; l'Associazione rimuove quanto controlla, fermo restando che copie, condivisioni e cache di terzi possono non essere integralmente recuperabili
- le testimonianze possono essere anonime, con solo nome o con nome e cognome secondo la scelta documentata della persona

8. Strumenti digitali e messaggistica

Strumento	Regola minima
Gmail, Drive, Forms e Classroom	account nominativi, cartelle per progetto, permessi limitati e rimozione degli accessi al termine
WhatsApp	comunicazioni operative; niente documenti d'identità o dati sanitari dettagliati, salvo minimo indispensabile in urgenza
Canva e strumenti creativi	contenuti già autorizzati o anonimizzati; nessun archivio parallelo di dati dei partecipanti
Piattaforme Erasmus+	solo dati richiesti dal programma e informazione alle persone sulle informative istituzionali applicabili
Moduli digitali	campi minimi, informativa collegata, accesso limitato e data di chiusura/cancellazione definita

Quando ragionevolmente possibile, chi non desidera entrare in un gruppo di messaggistica riceve un canale alternativo per le informazioni essenziali. I gruppi non vengono riutilizzati per finalità estranee al progetto.

9. Partner, fornitori e trasferimenti

Ai partner si comunicano normalmente soltanto nome, cognome, data di nascita e informazioni pratiche su allergie o intolleranze quando necessarie. Prima di ogni condivisione si definiscono ruolo, finalità, base giuridica, sicurezza, tempi e cancellazione. I fornitori che trattano dati per conto dell'Associazione sono vincolati, quando applicabile, da un accordo ai sensi dell'articolo 28 GDPR.

- la condivisione avviene con collegamenti limitati o canali concordati, non tramite cartelle pubbliche
- per trasferimenti fuori dallo Spazio economico europeo si verificano decisione di adeguatezza o garanzie applicabili e rischi del servizio
- il partner non può usare i dati per proprie campagne o finalità ulteriori senza una base autonoma e una propria informativa

10. Sicurezza e controllo degli accessi

- account personali, password robuste e autenticazione a più fattori dove disponibile
- accesso secondo necessità: normalmente Presidente e responsabile di progetto per i dati dei partecipanti
- cartelle separate per progetto e per dati sanitari, incidenti o safeguarding
- nessun inoltro automatico a email personali non autorizzate e nessun link aperto a chiunque

- dispositivi protetti da blocco, aggiornamenti e cancellazione remota quando disponibile
- verifica periodica degli accessi, revoca alla conclusione del compito e copie di sicurezza proporzionate
- stampa solo se necessaria, custodia chiusa e distruzione sicura

11. Conservazione e cancellazione

Ogni progetto indica tempi collegati alla finalità, agli obblighi legali, fiscali, assicurativi e del finanziatore. Le informazioni sanitarie, i contatti di emergenza e le copie di documenti vengono eliminate appena termina la necessità operativa; di regola alla chiusura del progetto. Le copie dei documenti d'identità non vengono conservate se non esiste una necessità specifica e documentata.

- documenti amministrativi, contrattuali e di rendicontazione seguono i termini applicabili
- consensi e revoche sono conservati quanto necessario a dimostrare le scelte e gestire gli usi autorizzati
- incidenti, reclami e safeguarding seguono un archivio riservato e tempi distinti basati su tutela e possibili pretese
- la chiusura comprende Drive, Forms, Classroom, download locali, email, dispositivi e copie cartacee

12. Diritti delle persone

Le persone possono chiedere accesso, rettifica, cancellazione, limitazione, portabilità quando applicabile, opposizione e revoca del consenso senza pregiudicare la liceità precedente. Possono inoltre proporre reclamo al Garante per la protezione dei dati personali.

> **TEMPI DI RISPOSTA**
> La richiesta viene registrata, l'identità verificata in modo proporzionato e la risposta fornita senza ingiustificato ritardo, normalmente entro un mese. Nei casi complessi il termine può essere esteso secondo il GDPR, informando la persona entro il primo mese.

13. Violazioni dei dati personali

> **SEGNALAZIONE IMMEDIATA**
> Chiunque perda un dispositivo, invii dati alla persona sbagliata, esponga un link, subisca un accesso anomalo o rilevi perdita, modifica o indisponibilità dei dati informa immediatamente il Presidente. Non cancella prove e non comunica autonomamente con interessati o autorità.

L'Associazione contiene l'evento, documenta fatti ed effetti e valuta il rischio per le persone. Quando richiesto, notifica il Garante senza ingiustificato ritardo e, ove possibile, entro 72 ore dalla conoscenza; se il rischio è elevato comunica anche alle persone coinvolte con linguaggio chiaro. Ogni violazione viene registrata, anche quando non è notificata, con la motivazione della decisione.

14. Intelligenza artificiale

- non si inseriscono in strumenti generativi dati identificativi, sanitari, di safeguarding o documenti dei partecipanti
- si usano dati anonimizzati, aggregati, sintetici o già destinati alla pubblicazione, verificando prima termini e impostazioni del servizio
- l'IA non decide selezioni, idoneità, supporti o misure disciplinari; ogni risultato viene verificato da una persona competente
- materiali, immagini e testimonianze non vengono usati per addestrare sistemi o creare imitazioni senza una base specifica e informazione chiara

15. Formazione, controllo e revisione

- ogni team riceve istruzioni proporzionate sui dati che utilizza e sui canali ammessi
- il registro delle attività di trattamento, i fornitori e gli accessi vengono riesaminati almeno annualmente
- nuovi strumenti, categorie particolari, monitoraggi sistematici o trattamenti ad alto rischio richiedono valutazione preventiva e, quando necessaria, una valutazione d'impatto
- la policy è revisionata ogni due anni e dopo violazioni, cambi normativi, nuovi Paesi, strumenti o attività

16. Contatti

Titolare	Io Per l'Altro - APS
Codice fiscale	97786260584
Sede	Via Agostino Scaparro 7, 00122 Roma
RUNTS	G09433
Email privacy e diritti	ipaostia@gmail.com
PEC	ioperlaltro@pec.it
Sito	www.ioperlaltro.com
Rappresentante legale	Marco Valerio Battaglia

17. Riferimenti

- Regolamento (UE) 2016/679 (GDPR), in particolare artt. 5, 6, 9, 12-22, 24-25, 28, 30, 32-35 e 44-49.
- D.Lgs. 196/2003, come modificato dal D.Lgs. 101/2018.
- Garante per la protezione dei dati personali: principi del trattamento, registro delle attività e data breach.
- Guida del Programma Erasmus+ 2026 e informative privacy delle piattaforme Erasmus+.

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

Approvazione

Approvata dal	Consiglio direttivo di Io Per l'Altro - APS
Data della delibera	30 agosto 2026
Entrata in vigore	1 ottobre 2026
Firma del legale rappresentante	Marco Valerio Bettaglia