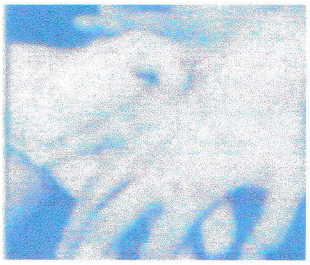

ASSOCIAZIONE DI VOLONTARIATO INSIEME ODV

DOCUMENTO SULLA TUTELA DEI DATI PERSONALI

Documento aggiornato al 29/04/2024

Approvato in sede di Assemblea dei soci il 29/04/2024

Documento redatto sulla base del GDPR
(GENERAL DATA PROTECTION REGULATION)
Regolamento(UE) 2016/679
del D.Lgs. n. 196/2003 aggiornato con D.Lgs. n. 101/2018
Adeguato alle nuove linee guida sui cookie e sugli altri sistemi di tracciamento, archiviazione delle informazioni
GPDP (Garante per la Protezione dei Dati Personali)
Provvedimento del 21 dicembre 2023)
(G.U. n. 163 del 9 luglio 2021)

Scopo del presente documento è quello di indicare il quadro delle misure di sicurezza organizzative, fisiche e logiche adottate e da adottare per il trattamento dei dati personali effettuato dall'Associazione di Volontariato INSIEME ODV (di seguito Associazione).

1. Elenco dei trattamenti di dati personali

L'Associazione raccoglie e utilizza comunemente, nello svolgimento della propria attività, dati personali, e cioè informazioni e notizie riferite:
a) ai propri soci/aderenti;
b) ai beneficiari dell'attività istituzionale o utenti del servizio;
c) ai consulenti e collaboratori esterni;
d) agli eventuali dipendenti;
e) agli enti pubblici;
f) agli altri ETS e in genere i soggetti con cui vengono a contatto;
g) alle persone, enti e aziende a cui indirizzare campagne di sensibilizzazione e fundraising, ecc.
h) agli utenti del proprio sito istituzionale e della pagina facebook.

L'Associazione tratta i seguenti dati:

1. **dati comuni di**:
   - soci
   - professionisti
   - fornitori

I dati comuni riguardano:
nome, data di nascita, numero di cellulare dei soci o beneficiari, dati ricavati o comunque ricavabili da albi, elenchi e registri che per legge sono pubblici;

2. **dati sensibili o, come definiti dal g.d.p.r. "particolari categorie di dati" di:**
   - fruitori dei servizi

I "dati particolari" riguardano (art. 9 DGPR)

- DATI SENSIBILI, che rivelano "l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale"
- DATI GENETICI e DATI BIOMETRICI intesi a identificare in modo univoco una persona fisica
- DATI SANITARI (e cioè i dati relativi alla salute) o quelli relativi alla vita sessuale o all'orientamento sessuale della persona.

I dati "particolari" riguardano la sfera più intima dell'individuo e pertanto richiedono una particolare protezione in quanto, se apprese al di fuori di un determinato contesto, possono essere causa di atteggiamenti discriminatori.
Per il trattamento dei dati "particolari", l'associazione dovrà attenersi :

- alle finalità del trattamento (art. 5 e 6 del Codice del Terzo Settore) sulle "attività di interesse generale" e sulla "attività diverse";
- alla possibilità di comunicare i dati del singolo socio anche agli altri soci solo se le modalità di tale comunicazione siano descritte nell'informativa ex art. 13 GDPR, e se vengano comunque rispettati i principi di necessità, finalità e minimizzazione (e venga comunque preferita la comunicazione individuale al socio laddove vengano in considerazione profili esclusivamente personali);
- alla comunicazione e diffusione dei dati sensibili all'esterno dell'associazione solo con il consenso degli interessati (tranne i dati sanitari e quei dati idonei a rivelare la vita sessuale i quali non saranno diffusi nemmeno su consenso dell'interessato), previa informativa e purché i dati siano strettamente pertinenti alle finalità ed agli scopi perseguiti.

3. Dati giudiziari

Sono dati giudiziari tutte le annotazioni (di natura penale) che risultano dal casellario giudiziale, tra cui le sentenze di condanna e i decreti penali irrevocabili, le misure di sicurezza poste a carico di un individuo, i provvedimenti di amnistia e ogni altro dato relativo "ai reati".

Non invece le sentenze e i provvedimenti civili.

Il trattamento di dati giudiziari è possibile solo se si rientra nelle ipotesi di liceità dell'art. 6 GDPR:

a) se il trattamento avviene "sotto il controllo dell'Autorità pubblica"

b) se il trattamento è autorizzato dal diritto dell'Unione o dal diritto italiano che prevedano garanzie appropriate per i diritti e le libertà degli interessati.

L'associazione è a contatto con dati giudiziari ogni qualvolta accoglie persone che hanno subito una condanna penale (ammessi a lavori di pubblica utilità quali sanzioni sostitutive di pene brevi o misure alternative alla detenzione) o persone che scelgono la "messa alla prova" come misure per evitare la condanna

2. Titolare del trattamento

Titolare del trattamento dei dati è l'Associazione di volontariato INSIEME ODV.

Le decisioni sui trattamenti da svolgere vanno adottate dall'organo o dalle persone fisiche cui è attribuita la gestione dell'ente (Consiglio Direttivo, Presidente).

Gli adempimenti richiesti dal GDPR devono essere attuati da persone fisiche (Presidente, consigliere delegato, dipendenti, o anche volontari);

Le responsabilità civili, amministrative e penali in caso di violazione del GDPR gravano prevalentemente sulle persone fisiche che hanno agito o hanno omesso di adottare le misure di sicurezza necessarie.

Obblighi del titolare del trattamento dati (l'art. 5 del GDPR)

L'Associazione si impegna a:

- trattare i dati in modo lecito e secondo correttezza e trasparenza;
- raccogliere i dati solo per finalità determinate, esplicite e legittime, ed utilizzare i dati solo in termini compatibili con tali scopi ("limitazione delle finalità") ;
- assicurarsi che i dati raccolti siano adeguati, pertinenti e non eccedenti rispetto a quanto necessario per il perseguimento delle finalità per cui sono raccolti ("minimizzazione dei dati");
- siano esatti e, se necessario, costantemente aggiornati ("esattezza dei dati");
- conservarli per un periodo di tempo non superiore a quello necessario per il raggiungimento delle finalità per cui sono stati raccolti, a meno che la conservazione non avvenga per fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici ("limitazione della conservazione");
- garantire un'adeguata sicurezza e protezione dei dati personali, mediante misure tecniche e organizzative adeguate, per evitare trattamenti non autorizzati o illeciti e per evitare la perdita e la distruzione accidentale dei dati ("integrità e riservatezza")

Come va richiesto il consenso per i dati comuni e i dati "particolari"

L'associazione consegna all'interessato una informativa (allegata o contenuta nella domanda di adesione all'associazione) che sottoscriverà nel momento stesso in cui consegna i suoi dati.

Se i dati non sono forniti dall'interessato ma da altre persone/soggetti, l'obbligo dell'informativa all'interessato va adempiuto, ai sensi dell'art. 14 comma 3 GDPR, entro un mese o nel momento in cui i dati vengono comunicati per la prima volta all'interessato o a terzi.

Se i dati sono forniti attraverso web sarà utilizzato il point&click, nella quale l'interessato può accedere per fornire i propri dati personali, per essere informato delle modalità del trattamento, e soprattutto per autorizzare il trattamento barrando una o più caselle.
All'informativa si accompagna la richiesta di consenso al trattamento dei dati che l'interessato deve sottoscrivere.
Con riferimento agli interessati che siano MINORENNI, il consenso va prestato da coloro che esercitano la responsabilità genitoriale o, se esiste, dal tutore.
I dati dei soci che hanno lasciato l'Associazione verranno utilizzati nell'ambito dell'attività dell'Associazione senza comunicazione all'esterno (per tale comunicazione ci vuole il consenso specifico dell'ex socio) e saranno strettamente inerenti alle specifiche attività "residue" (es. invio della newsletter, convocazione per gli anniversari, ecc.) come citato dall'art. 9 comma 2 lett. d) del GDPR.
I dati dei soci fruitori dei servizi offerti dall'associazione saranno cancellati quando l'attività o il servizio nei loro confronti debba intendersi definitivamente esaurito.

Diritti dell'interessato:

L'interessato del trattamento può chiedere al Titolare:
- di avere conferma che l'Ente utilizza i suoi dati e di sapere quali siano questi dati;
- di conoscere l'origine dei dati (cioè come e da chi l'associazione li ha acquisiti), le finalità del trattamento, i soggetti a cui i dati vengono comunicati e il periodo di conservazione dei dati;
- di rettificare (correggere o integrare) i dati inesatti o incompleti;
- di cancellare i dati (cd. diritto "all'oblio") quando il trattamento non è più necessario per il raggiungimento delle finalità per cui sono stati raccolti, o in caso di revoca del consenso, o in caso di trattamento illecito o negli altri casi previsti dall'art. 17 GDPR;
- di ottenere una "limitazione del trattamento" nei casi previsti dall'art. 18 GDPR;
- di poter trasferire i dati ad un altro titolare (diritto "alla portabilità dei dati");
- di opporsi al trattamento dei suoi dati, anche se svolto correttamente dall'associazione, se sussistono "motivi particolari" (se il trattamento, anche se lecito, risulta lesivo della sua dignità o riservatezza);
- di opporsi al trattamento dei dati svolto per il "marketing diretto" (invio di materiale pubblicitario o vendita diretta o compimento di ricerche di mercato o di comunicazione commerciale);

3. Responsabile della Protezione dei Dati - Data Protection Officer (RPD/DPO)

Il Responsabile della Protezione (o Data Protection Officer) dei dati ha compiti di controllo e assistenza sui trattamenti svolti dal Titolare, al fine di assicurare che tali trattamenti siano conformi al GDPR.
Egli viene nominato dai membri del C.d.A. e svolge le funzioni di responsabile della protezione dei dati personali, come definite dall'art. 39 RGDP tra cui:

- informare e consigliare il controllore e i volontari che effettuano operazioni di trattamento in merito ai loro obblighi ai sensi del RGDP e di altre disposizioni applicabili in materia di protezione dei dati;
- controllare il rispetto del RGDP, delle altre disposizioni applicabili in materia di protezione dei dati e dei provvedimenti del Titolare per la protezione dei dati personali, compresa l'allocazione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento e le relative verifiche;
- su richiesta, fornire consulenza in relazione alla valutazione d'impatto sulla protezione dei dati e alla sua attuazione ai sensi dell'art. 35 RGDP;
- collaborare con l'autorità di controllo e fungere da punto di contatto per l'autorità di controllo su questioni relative al trattamento, compresa la consultazione preventiva sulla valutazione d'impatto in materia di protezione dei dati a norma dell'art. 36 del RGDP e, se del caso, fornire consulenza su tutte le altre questioni;
- fungere da punto di contatto per l'esercizio dei diritti degli interessati a norma degli artt. 12-23 RGDP ed evadere le loro richieste relative alle attività di trattamento.

Ai sensi dell'art. 38 RGDP, nell'esercizio delle proprie funzioni il DPO:

- deve sempre riferire al più alto livello direttivo del Titolare;
- non gode di alcun potere di rappresentare il Titolare;
- non può essere soggetto a poteri direttivi o istruzioni del Titolare;
- deve essere sempre dotato dei mezzi necessari ed idonei al corretto svolgimento dei propri compiti ed al mantenimento e costante aggiornamento delle proprie conoscenze, anche in termini di personale e risorse economiche;
- deve sempre essere coinvolto dal Titolare in tutte le questioni relative alla protezione di dati personali;
- non deve svolgere la propria funzione di DPO in conflitto di interessi.

4. Responsabile interno del trattamento dei dati

Il Responsabile del trattamento dei dati svolge, su incarico scritto del Titolare o sulla base di un contratto, un trattamento dei dati "per conto" del Titolare.
Il Responsabile ha il compito di compiere tutto quanto si renderà necessario ai fini di assicurare il rispetto e la corretta applicazione, da parte dell'Associazione, degli obblighi, disposizioni e principi di cui al GDPR e del D.Lgs. n. 196 del 30.6.2003
Il Responsabile:

- nomina o fa nominare per iscritto dal Titolare gli Incaricati del trattamento, fornendo loro istruzioni operative e vigilando sul rispetto di dette istruzioni;
- individua i Responsabili (esterni) del trattamento ai sensi dell'art. 28 GDPR e propone al Titolare la stipula del relativo Accordo/contratto;
- classifica le banche dati e propone al Titolare un sistema complessivo di trattamento dei dati personali, comuni e "particolari", dell'Associazione;
- collabora con la ditta incaricata della manutenzione e aggiornamento delle banche dati informatiche e del sistema informatico al fine di assicurare, ai sensi dell'art. 32 GDPR, l'adozione e la conservazione di misure e procedure informatiche adeguate e vigilare sul rispetto di dette misure da parte degli Incaricati, al fine di impedire trattamenti non autorizzati o illeciti o la perdita, la distruzione o il danno accidentale delle banche dati o dei dati personali;
- attua e fa eseguire gli obblighi di informativa ex art. 13 e 14 GDPR e di acquisizione del consenso degli interessati ex art. 7, 8, 9 e 10 GDPR;
- garantisce all'interessato l'effettivo esercizio dei diritti previsti dagli artt. 15, 16, 17, 18, 20, 21 GDPR;
- redige e tiene aggiornato il Registro dei Trattamenti di cui all'art. 30 GDPR;
- da immediata comunicazione al Titolare e all'eventuale esperto informatico o ditta incaricata nel caso sospetti o riscontri un problema di sicurezza relativamente al trattamento dei dati personali;

Il Responsabile assicura che il trattamento dei dati all'interno dell'Associazione avvenga nel rispetto dei principi e delle disposizioni di cui al Capo II del GDPR, ed in particolare che:

- i dati siano trattati in modo lecito, corretto e trasparente
- i dati siano raccolti solo per le specifiche finalità del trattamento assegnato (principio di limitazione delle finalità)
- i dati siano adeguati, pertinenti e non eccedenti rispetto alle finalità (principio di minimizzazione dei dati)
- i dati siano esatti e se necessario aggiornati (principio di esattezza dei dati), predisponendo eventuali direttive in ordine al loro aggiornamento;
- i dati siano conservati per un periodo non superiore a quello necessario al raggiungimento delle finalità del trattamento (principio della limitazione della conservazione), impartendo eventuali ulteriori istruzioni in ordine alla cancellazione o alla anonimizzazione/minimizzazione.
- organizza la formazione degli Incaricati in materia di protezione dei dati personali;
- garantisce la massima riservatezza e discrezione circa le caratteristiche generali e i dettagli particolari delle mansioni affidategli in ordine ai trattamenti di dati e non divulgare, neanche

dopo la cessazione dell'incarico, alcuna delle informazioni di cui è venuto a conoscenza;
- adotta, per ogni operazione di trattamento svolta in prima persona, le misure di sicurezza a cui è tenuto ciascun Incaricato.

5. Come vengono conservati i dati

I dati vengono trattati e conservati in fascicoli riposti in apposito armadio dotato di chiusura, nonché trattati tramite computer portatile provvisto di collegamento ad internet.
La sede dell'Associazione ove vengono trattati i dati, è situata in zona non centrale, in uno stabile dove sono collocate le sedi operative di altre associazioni, è dotata di una porta di ingresso allo stabile e di una di ingresso alla sede.
Il rischio di accesso alle singole stanze dell'Associazione può essere definito medio, atteso che l'ingresso di terzi estranei avviene solo previa accettazione e controllo presso la sala d'attesa.
Il rischio di acceso allo strumento informatico da parte di persone non autorizzate può essere definito basso, essendo lo stesso facilmente rimovibile e tenuto sotto stretto controllo dal responsabile del trattamento.

MISURE DI SICUREZZA

Per il trattamento informatico dei dati:

- somministrazione di istruzioni scritte/lettere di incarico alle persone che all'interno dell'Associazione trattano dati personali (nominative o per categorie di soggetti: es. volontari, soci, dirigenti, ecc.) sull'ambito del trattamento consentito a ciascun incaricato/categoria e sulle modalità del trattamento (cd. Sistema di autorizzazione)
- Attribuzione di credenziali di autenticazione a ciascun incaricato che utilizza il computer (generalmente username e password) che gli consentano di accedere al computer e di svolgere i trattamenti a lui consentiti
- dotazione di idonei e aggiornati sistemi di protezione (antivirus, firewall, aggiornamento dei sistemi operativi e dei programmi, salvataggio dei dati in supporti esterni o in altri server, ecc.) agli strumenti informatici dell'Associazione

E' disposto che lo strumento elettronico non venga lasciato incustodito e reso accessibile a terzi. A tale riguardo, per evitare errori e dimenticanze, è stato inserito lo screensever dopo un minuto di non utilizzo.
Per il trattamento cartaceo dei dati (libro dei soci, il libro dei volontari, la rubrica per la corrispondenza):

- somministrazione di istruzioni scritte/lettere di incarico (nominative o per categorie di soggetti: es. volontari, soci, dirigenti, ecc.) sull'ambito del trattamento consentito a ciascun incaricato/categoria, sulle modalità di controllo e di custodia degli atti, dei documenti e dei fascicoli alle persone che all'interno dell'Associazione trattano dati personali;
- formazione rivolta ai consiglieri, ai volontari e in genere agli incaricati del trattamento sugli obblighi derivanti dal GDPR, conservandone la relativa documentazione

6. Sito Internet e piattaforme social

L'Associazione utilizza il sito internet www.insiemecenturipe.it e le piattaforme social Facebook e Instagram.

- **Sito Internet**

Il sito internet www.insiemecenturipe.it, per impostazione predefinita, al momento del primo accesso dell'utente, non utilizza nessun *cookie* diverso da quelli tecnici
I dati vengono trattati in relazione a ciascuna specifica finalità del trattamento e l'utilizzo di informazioni per l'accesso è limitato al minimo indispensabile per consentirne la fruizione. E' rimesso interamente all'interessato un effettivo, concreto potere di scelta in ordine alla possibilità di consentire o meno un utilizzo eventualmente più ampio dei suoi dati.
All'utente del sito sarà fornita una informativa breve che compare attraverso un **banner** non appena entra sul sito internet dove è specificato:
– se il sito utilizza cookie di profilazione
– l'indicazione relativa alla facoltà dell'utente di accettare l'installazione di tutti i cookie, rifiutare detta istallazione (attraverso una x nella casella apposita) di scegliere le categorie di cookie attraverso il rimando ad una specifica area.
– il *link* alla menzionata area nella quale poter scegliere in modo analitico le funzionalità, le *terze parti* e i *cookie* che si vogliono installare e poter prestare il consenso all'impiego di tutti i *cookie* se non dato in precedenza o revocarlo, anche in unica soluzione, se già espresso.
– l'indicazione del fatto che chiudendo il banner senza accettare, resteranno installati solo i cookie tecnici necessarie.
– l'indicazione di un link di rinvio alla pagina in cui si trova l'informativa estesa.
- il banner resta evidente finché non viene operata una scelta da parte dell'utente e, fintantoché questa scelta non viene effettuata, resteranno installati esclusivamente i cookie tecnici.
- una volta effettuata la scelta, il banner scompare per sei mesi, a meno che mutano significativamente le condizioni del trattamento oppure è impossibile, per il sito, sapere se un cookie sia stato già memorizzato nel dispositivo.
– E' presente un registro dei consensi.

L'accesso a informazioni già archiviate sono consentiti unicamente a condizione che il contraente o l'utente abbia espresso il proprio consenso dopo essere stato informato con modalità semplificate (art. 122 Codice della privacy)

L'informativa estesa contiene le seguenti informazioni:

- l'identità e i dati di contatto del titolare del trattamento
- i dati di contatto del responsabile della protezione dei dati
- le finalità del trattamento cui sono destinati i dati personali
- i legittimi interessi perseguiti dal titolare del trattamento o da terzi
- il periodo di conservazione dei dati
- il diritto di revocare il consenso in qualsiasi momento
- il diritto di proporre reclamo a un'autorità di controllo

Deve contenere, inoltre:
- la natura facoltativa o obbligatoria dei dati raccolti e le conseguenze per l'utente di un suo eventuale diniego a fornire i dati.
- la possibilità per l'utente di manifestare le proprie opzioni in merito all'uso dei cookie da parte del sito
- elenca i cookie utilizzati e le singole e relative finalità
  - **cookies tecnici** - navigazione, lingua, carrello e-commerce, autenticazione (solo informativa estesa con il link diretto dall'home page)
  - **cookies analytics propri** - assimilati ai cookie tecnici
  - **cookies analytics di terzi** (come Google Analytics) - consenso alla loro installazione (nell'informativa

breve c'è il pulsante per accettare tutti i cookie, quello per rifiutarli tutti e quello per selezionare le categorie di cookie che si vogliono installare)
- **cookies di profilazione propria** - assimilati ai cookie tecnici
- **cookies di profilazione altrui** (come Adsense ads) - informativa breve con banner semplificato di consenso espresso tramite il quale si avverte che il sito consente l'invio di cookies di profilazione di terze parti + link ad informativa completa ex art. 13 GDPR, il pulsante per accettare tutti i cookie, quello per rifiutarli tutti e quello per selezionare le categorie di cookie che si vogliono installare.

7. Data breach

Il "Data Breach" o "violazione dei dati personali" (art. 4 e 33 GDPR) è una "violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzato o l'accesso ai dati personali". E' la perdita, il danneggiamento o la fuoriuscita di dati o l'accesso illecito anche indipendente dalla volontà dell'Associazione (perdita di una chiavetta USB, furto del PC, cancellazione di un archivio dati, accesso al computer di estranei, ecc.).
In caso di data breach, il Titolare(art. 33 e 34):
a) denuncia/notifica al Garante per la Protezione dei Dati Personali l'esistenza della violazione "senza giustificato ritardo e se possibile entro 72 ore" dal momento in cui il Titolare ha conoscenza della violazione medesima. L'obbligo di denuncia non sussiste quando sia improbabile che la violazione comporti un rischio/pregiudizio per i diritti e le libertà delle persone (ad esempio se si tratta di dati comuni, o se la violazione consiste nella mera distruzione di dati che possono essere richiesti all'interessato);
b) comunica la violazione all'interessato "senza ingiustificato ritardo", l'esistenza della violazione che riguarda i suoi dati. L'obbligo di comunicazione non sussiste, anche in questo caso, quando la violazione non comporta un rischio/pregiudizio per i diritti e le libertà dell'interessato, e anche negli altri casi di cui all'art. 34 GDPR (ad esempio quanto il Titolare è riuscito ad evitare la lesione dei diritti o la comunicazione richiede sforzi sproporzionati per l'esistenza di un gran numero di interessati).

Il Titolare ha l'obbligo di responsabilizzare e formare Consiglieri, volontari e dipendenti sui rischi di data breach.
Se un Socio, un volontario, un dipendente, un consigliere è venuto a conoscenza di un data breach, è tenuto ad informare **immediatamente** il Titolare (Presidente)

La Presidente dell'Associazione

INSIEME ODV

dott.ssa Prospera Longo

La Responsabile della Protezione dei Dati –(RPD)
Data Protection Officer (DPO

sig.ra Filippa Barbagallo