

INFORMATIVA SULLA PRIVACY

Sistema Gestione Emergenze (SGE)

Versione: 1.0 — [data]

Sito: <https://sge.hathost.cloud>

App mobile: SGE (iOS / Android)

1. Titolare del trattamento

Il Titolare del trattamento dei dati personali trattati tramite SGE è:

NetPro IT Solution SRL

Indirizzo: Via San Filippo Neri 22A, 16035 Rapallo (GE)

Email: info@netproit.it

PEC: info@pec.netproit.it

Telefono: +39 0287189457

Ogni ente convenzionato può essere titolare autonomo per i dati di propria competenza.

2. Responsabile del trattamento / Fornitore della piattaforma

La piattaforma tecnologica SGE è sviluppata e gestita da:

NetPro IT Solution SRL

Email: info@netproit.it

Telefono: +39 0287189457

NetPro IT Solution SRL opera, ove applicabile, quale Responsabile del trattamento ex art. 28 GDPR per conto del Titolare, secondo accordo di nomina a Responsabile del trattamento (DPA).

Hosting infrastruttura: NetPro IT Solution SRL — server ubicati in EU nello specifico a Milano (IT) con ridondanza a Francoforte (DE).

3. Responsabile della Protezione dei Dati (DPO)

Contatto DPO: Non nominato

In assenza di DPO obbligatorio, per richieste privacy: privacy@netproit.it .

4. Ambito di applicazione

La presente informativa riguarda il trattamento dei dati personali effettuato tramite:

- portale web SGE (accesso operatori, enti, amministratori);
- API backend del sistema;
- applicazione mobile SGE per operatori autorizzati;
- moduli pubblici (es. registrazione cittadini agli avvisi, caricamento allegati tramite link temporaneo);

- servizi collegati (notifiche email, push, Telegram, integrazioni meteo).

SGE non è un servizio di emergenza pubblica (112/115/118): è uno strumento di coordinamento per Protezione Civile, comuni, associazioni ed enti autorizzati.

5. Tipologie di interessati e dati trattati

5.1 Operatori e utenti registrati (ruoli COC, associazioni, enti, admin)

Dati identificativi e di contatto: nome, cognome, email, eventuale codice fiscale, ID Telegram (se configurato).

Dati di autenticazione e sicurezza: password (conservata in forma crittografata), token di sessione (JWT), eventuale segreto e codici di backup per autenticazione a due fattori (2FA), credenziali passkey/WebAuthn (identificativi tecnici del dispositivo, non dati biometrici).

Dati di profilo operativo: ruoli, permessi, associazione/ente di appartenenza, comuni e sezioni abilitati.

Dati tecnici: token push del dispositivo mobile (APNs/FCM), indirizzo IP, log di accesso e attività (se abilitati), timestamp di utilizzo.

5.2 Volontari e personale operativo degli enti

Oltre ai dati sopra, possono essere trattati: data e luogo di nascita, sesso, codice fiscale, recapiti telefonici, indirizzo di residenza, qualifiche/formazione, note operative, stato operativo (PC, AIB, ecc.), eventuale collegamento a account utente.

5.3 Cittadini iscritti agli avvisi comunali

Tramite modulo di registrazione volontaria possono essere trattati: nome, cognome, telefono, email, indirizzo, coordinate geografiche (se fornite), note per emergenza (es. esigenze particolari), ID Telegram (opzionale), token per notifiche push (Firebase), stato di verifica email.

Nota sulle categorie particolari: le “note per emergenza” possono contenere informazioni relative alla salute o ad altre categorie particolari di dati (art. 9 GDPR). Il conferimento è facoltativo; la base giuridica è indicata al § 6.

5.4 Segnalanti e soggetti coinvolti nelle operazioni

Durante eventi ed emergenze possono essere trattati dati relativi a segnalazioni (descrizione, indirizzo, coordinate GPS, gravità, note), allegati fotografici/video, comunicazioni radio/telefoniche (nome segnalante/chiamante, contenuto messaggio), interventi e squadre sul campo.

5.5 Caricamento allegati tramite link pubblico

Chi riceve un link temporaneo può caricare file (immagini, video, documenti) collegati a una segnalazione senza creare un account. Possono essere trattati metadati del file, contenuto dell'allegato e dati tecnici di connessione (IP, user agent) per sicurezza e tracciabilità limitata.

6. Finalità e basi giuridiche del trattamento

Finalità	Base giuridica (art. 6 GDPR)
Erogazione del servizio SGE agli utenti autorizzati (login, gestione profilo, ruoli)	Esecuzione di misure precontrattuali/contrattuali (lett. b); legittimo interesse alla sicurezza del sistema (lett. f)
Coordinamento operativo di emergenze ed eventi (segnalazioni, squadre, interventi, mappe)	Adempimento di compiti di interesse pubblico rilevante / tutela di interessi vitali in situazioni di emergenza (lett. e/d), ove applicabile
Gestione anagrafica volontari e risorse degli enti	Contratto/rapporto associativo o obbligo di legge in materia di Protezione Civile (lett. b/c)
Registrazione volontaria cittadini agli avvisi comunali	Consenso dell'interessato (lett. a), revocabile in qualsiasi momento
Invio avvisi, alert meteo e notifiche operative (email, push, Telegram)	Consenso (cittadini) o legittimo interesse/interesse pubblico (operatori e volontari autorizzati)
Geolocalizzazione segnalazioni e posizione squadre	Esecuzione del servizio richiesto dall'operatore; interesse pubblico nella gestione dell'emergenza
Autenticazione rafforzata (2FA, passkey)	Legittimo interesse / obblighi di sicurezza
Log di sistema, audit e prevenzione abusi	Legittimo interesse alla sicurezza informatica (lett. f)
Adempimenti di legge e difesa in giudizio	Obbligo di legge (lett. c) / legittimo interesse (lett. f)

Categorie particolari di dati (art. 9): ove presenti nelle note di emergenza o nelle segnalazioni, il trattamento si basa, a seconda dei casi, su consenso esplicito, interessi vitali, finalità di medicina preventiva/soccorso, o motivi di rilevante interesse pubblico con adeguate garanzie, come previsto dall'art. 9, par. 2 GDPR e dalla normativa nazionale applicabile.

7. Modalità del trattamento

I dati sono trattati con strumenti informatici e telematici, con logiche strettamente correlate alle finalità indicate, e con misure di sicurezza tecniche e organizzative adeguate, tra cui:

- comunicazioni cifrate (HTTPS/TLS);

- hash delle password (bcrypt);
- controllo accessi basato su ruoli (RBAC);
- token di sessione con scadenza;
- autenticazione a due fattori e passkey (opzionali);
- limitazione dei rate sulle API pubbliche;
- backup periodici del database (*se attivati dal Titolare*);
- accesso ai dati di popolazione protetta tramite password master dedicata (solo profili autorizzati).

8. Destinatari e categorie di destinatari

I dati possono essere comunicati, nei limiti delle finalità, a:

- Personale autorizzato del Titolare e degli enti convenzionati (COC, associazioni, enti);
- NetPro IT Solution SRL e personale tecnico autorizzato (manutenzione piattaforma);
 - Fornitori di servizi che operano come responsabili del trattamento, tra cui:
 - provider di hosting e infrastruttura cloud;
 - servizi email (SMTP configurato dal Titolare);
 - Apple Push Notification service (APNs) per notifiche app iOS;
 - Google Firebase Cloud Messaging (FCM) per notifiche push (es. cittadini Android);
 - Telegram (solo se l'interessato ha fornito volontariamente l'ID Telegram e il bot è attivo);
 - fornitori di servizi meteo (Regione Liguria, reti meteo collegate — generalmente senza trasmissione di dati personali degli utenti).

Non è prevista la vendita dei dati personali a terzi.

Non è previsto il profilazione automatizzata che produca effetti giuridici significativi sull'interessato.

9. Trasferimenti verso Paesi extra UE

I fornitori indicati (es. Apple, Google, Telegram) possono trattare dati anche extra UE. Tali trasferimenti avvengono, ove necessario, sulla base di decisioni di adeguatezza o clausole contrattuali standard approvate dalla Commissione Europea, nonché misure supplementari ove richieste.

10. Periodo di conservazione

I dati sono conservati per il tempo necessario alle finalità per cui sono stati raccolti:

- Account operatori/volontari: per tutta la durata del rapporto e, successivamente, per il periodo previsto da obblighi di legge o tutela dei diritti del Titolare (in genere fino a [X] anni, salvo diversa normativa).

- Eventi, segnalazioni, log operativi: per la durata dell'emergenza e per un periodo successivo di archiviazione/configurabile dal Titolare (es. chiusura automatica eventi dopo N giorni — parametro di sistema).
- Registrazioni cittadini agli avvisi: fino a revoca del consenso, cancellazione da parte dell'interessato o cessazione del servizio da parte del comune.
- Token push e log tecnici: per il tempo strettamente necessario all'erogazione del servizio e alla sicurezza (in genere fino a disinstallazione app / logout / invalidazione token).
- Allegati su segnalazioni: collegati al ciclo di vita della segnalazione/evento.

Al termine dei periodi indicati, i dati sono cancellati, anonimizzati o conservati in forma aggregata, salvo obblighi di legge diversi.

11. Natura del conferimento e conseguenze del rifiuto

- Per operatori autorizzati, il conferimento di dati identificativi e credenziali è necessario per accedere al sistema; il rifiuto impedisce l'utilizzo del servizio.
- Per cittadini, la registrazione agli avvisi è facoltativa; il mancato conferimento impedisce di ricevere notifiche tramite SGE, ma non pregiudica l'accesso ai servizi di emergenza pubblica.
- Per geolocalizzazione, fotocamera e notifiche push sull'app mobile, il consenso del dispositivo è richiesto dal sistema operativo; alcune funzioni possono non essere disponibili senza tali permessi.

12. Diritti dell'interessato

Ai sensi degli artt. 15–22 GDPR, l'interessato ha diritto di:

- accesso ai propri dati;
- rettifica di dati inesatti;
- cancellazione ("diritto all'oblio"), nei casi previsti;
- limitazione del trattamento;
- portabilità dei dati, ove applicabile;
- opposizione al trattamento basato su legittimo interesse;
- revoca del consenso in qualsiasi momento (senza pregiudicare la liceità del trattamento precedente).

Cittadini registrati possono esercitare aggiornamento/cancellazione anche tramite le funzioni previste dal portale (link di modifica/cancellazione via email, ove attive).

Le richieste vanno inviate a: [email privacy / PEC del Titolare].

Il Titolare risponde entro 30 giorni (prorogabili nei casi previsti dalla legge).

13. Reclamo all'Autorità di controllo

L'interessato ha diritto di proporre reclamo al Garante per la Protezione dei Dati Personali (www.garanteprivacy.it) se ritiene che il trattamento violi il GDPR.

14. Cookie e tecnologie simili (portale web)

Il portale web utilizza:

- cookie/session storage necessari per l'autenticazione (token di sessione) e il funzionamento dell'applicazione;
- preferenze locali (es. tema chiaro/scuro) memorizzate nel browser;
- eventuali cookie tecnici di sicurezza.

(Se in futuro aggiungerete analytics o cookie non tecnici, va preparata una Cookie Policy separata e un banner di consenso.)

L'app mobile iOS/Android memorizza il token di sessione nel Keychain/Keystore del dispositivo e preferenze locali (ruolo selezionato, comune, ecc.).

15. Sicurezza specifica app mobile

L'app SGE per operatori può richiedere l'accesso a:

- Posizione: geolocalizzazione segnalazioni e aggiornamento posizione squadre;
- Fotocamera/Galleria: allegati alle segnalazioni;
- Face ID/Touch ID: solo per passkey (opzionale);
- Notifiche push: per alert operativi e meteo.

Tali permessi sono richiesti solo quando l'utente utilizza le relative funzioni o le abilita esplicitamente.

16. Minori

Il servizio di registrazione cittadini e l'accesso operativo non sono destinati a minori di 14 anni senza consenso del genitore/tutore. Gli account operatori sono riservati a soggetti autorizzati dagli enti titolari.

17. Modifiche all'informativa

Il Titolare può aggiornare la presente informativa. La versione vigente è pubblicata su [URL pagina privacy]. Per modifiche sostanziali, gli interessati registrati potranno essere informati con modalità appropriate.

18. Riferimenti normativi

Regolamento (UE) 2016/679 (GDPR), D.Lgs. 196/2003 e s.m.i. (Codice Privacy), normativa nazionale e regionale in materia di Protezione Civile, ove applicabile.