Nomina a responsabile del trattamento (art. 28 GDPR)

Versione 2026-09 · documento generato il 28/09/2026 da https://demo.antincendio.it

Questo documento è l'accordo previsto dall'**art. 28 del Reg. UE 2016/679 (GDPR)** fra te e noi, e vale quando usi il **registro antincendio**. Ne sei parte perché nel registro inserisci dati di altre persone: i tuoi addetti antincendio, le persone della tua organizzazione che accedono, i tecnici che firmano i verbali.

Per quei dati il **titolare del trattamento sei tu**: sono tuoi, decidi tu perché e per quanto tempo trattarli. Noi — **Automa S.r.l.**, c.f. e p.iva 16208401006, Via degli Olmetti 44/B int. C14, 00060 Formello (RM) — li trattiamo **per tuo conto**, e siamo il tuo *responsabile del trattamento*.

Accettando le condizioni di servizio (https://demo.antincendio.it/condizioni-di-servizio/) accetti anche questo accordo, che ne è parte integrante e porta la stessa versione. Se la tua organizzazione richiede un documento sottoscritto, scrivici a info@antincendio.it e te lo forniamo con lo stesso contenuto.

Questo accordo non riguarda: i dati che tratti tu direttamente come titolare fuori dalla piattaforma; le richieste di preventivo, dove il titolare siamo noi e i fornitori sono titolari autonomi (lo dice l'informativa privacy (https://demo.antincendio.it/privacy-policy/)); i dati del tuo account e della fatturazione, dove il titolare siamo noi.

1. Che cosa trattiamo per te

Oggetto e natura. Conservazione e organizzazione dei dati che inserisci nel registro antincendio, per il tempo in cui usi il servizio. Le operazioni sono: raccolta, registrazione, conservazione, consultazione, estrazione, cancellazione, e l'invio delle comunicazioni di servizio che chiedi.

Finalità. Erogarti il servizio: tenuta del registro dei presidi e dei controlli, calcolo delle scadenze, promemoria via email, generazione del registro in PDF, condivisione con il manutentore che *tu* incarichi, assistenza quando la chiedi.

Categorie di interessati. Le persone della tua organizzazione che accedono al registro; gli addetti antincendio che vi inserisci; i tecnici, tuoi o del manutentore, che eseguono e firmano i controlli.

Categorie di dati. Dati identificativi e di contatto (nome, cognome, indirizzo email); dati sulla formazione degli addetti antincendio (livello, ente, date di attestato e aggiornamento, idoneità tecnica); il nome di chi firma ciascun verbale; i dati tecnici delle sedi e dei presidi; le eventuali fotografie che alleghi ai verbali; i dati di accesso e i log tecnici.

Categorie particolari. Il servizio **non è progettato per dati particolari** (art. 9) né giudiziari: non inserirne. Se lo fai, resta una tua scelta e una tua responsabilità.

Durata. Fino alla cessazione del rapporto, e poi per il tempo indicato al punto 8.

2. Le nostre istruzioni sono le tue

Trattiamo i dati **solo su tua istruzione documentata**. Le istruzioni sono: questo accordo, le condizioni di servizio, e le azioni che compi tu o le persone che autorizzi dentro la piattaforma. Non usiamo i tuoi dati per finalità nostre: non li vendiamo, non li cediamo, non li usiamo per profilazione né per addestrare sistemi automatici.

Se un'istruzione ci sembra violare il GDPR o un'altra norma sulla protezione dei dati, te lo diciamo subito e possiamo sospenderne l'esecuzione.

Se una legge ci obbliga a un trattamento diverso, te ne informiamo prima di procedere, salvo che quella stessa legge lo vieti per motivi di interesse pubblico.

3. Chi, da noi, può vedere i tuoi dati

Solo le persone che ne hanno bisogno per lavorare al servizio, autorizzate per iscritto e vincolate alla riservatezza.

Il nostro personale di assistenza vede i **dati operativi** della tua organizzazione — sedi, presidi, scadenze, chi sono le persone che vi accedono — e **non vede i dati dei tuoi addetti**, che restano fuori dagli strumenti di back-office. Non può scrivere nel tuo registro: registrare o annullare un verbale è possibile solo a chi è membro della tua organizzazione o al manutentore che hai incaricato. Questa separazione è nel software, non è una promessa organizzativa.

4. Come li proteggiamo (art. 32)

Le misure in atto, in concreto:

- **Trasporto cifrato** (HTTPS/TLS) su ogni pagina e ogni chiamata verso i nostri fornitori; dati cifrati a riposo dai provider di database e archiviazione.
- **Separazione fra clienti a due strati**: l'autorizzazione applicativa, e — indipendentemente da essa — le politiche di sicurezza a livello di riga del database, che valgono per l'utenza con cui l'applicazione accede ai dati. Quell'utenza non può aggirarle, e l'applicazione lo verifica a ogni avvio: se non fosse così, si rifiuterebbe di partire. Una svista nel codice non basta a far vedere a un cliente i dati di un altro: servirebbero due errori indipendenti.
- **Sessioni firmate e revocabili**: la revoca di un accesso ha effetto immediato su tutti i dispositivi.
- **File caricati** (le foto dei verbali) validati sul contenuto, ricodificati — il che elimina anche i metadati, compresa la posizione GPS — conservati in un archivio privato nell'Unione Europea e accessibili solo con collegamenti firmati che scadono in pochi minuti.
- **Registro dei controlli in sola aggiunta**: un verbale non si modifica e non si cancella, si annulla con il motivo e resta tracciato.
- **Backup giornalieri** in un archivio separato nell'Unione Europea, con conservazione scalare (14 giornalieri, 8 settimanali, 12 mensili) e una **prova di ripristino automatica ogni mese**, che verifica anche che le misure di separazione fra clienti siano integre nel backup.
- **Verifiche automatiche delle difese** a ogni modifica del software: se una protezione viene rimossa, la pubblicazione si blocca.
- **Registrazione degli eventi** tecnici e monitoraggio degli errori, senza dati personali nei rapporti di errore.

Le misure possono cambiare nel tempo: possiamo sostituirle solo con misure di livello di sicurezza equivalente o superiore.

5. I fornitori di cui ci serviamo (sub-responsabili)

Ci autorizzi ad avvalerci dei fornitori elencati qui sotto, ciascuno vincolato da obblighi non meno onerosi di quelli di questo accordo. Sono infrastruttura: nessuno di loro usa i tuoi dati per sé.

- **Render** — applicazione e database, regione *Frankfurt* (Germania, UE).
- **Cloudflare** — rete, protezione dagli abusi, archiviazione dei file e dei backup con residenza nell'Unione Europea.
- **Resend** — invio delle email di servizio (promemoria, avvisi, reimpostazione della password). Il fornitore ha sede negli Stati Uniti: il trasferimento avviene sulla base delle clausole contrattuali tipo della Commissione europea. I dati coinvolti sono l'indirizzo email del destinatario e il contenuto del messaggio.
- **Sentry** — rilevazione degli errori tecnici, configurato per non raccogliere dati personali.

Se aggiungiamo o sostituiamo un fornitore, aggiorniamo questa pagina e te lo comunichiamo via email con almeno **trenta giorni** di preavviso. In quel periodo puoi opporti per motivi ragionevoli e legati alla protezione dei dati: se non troviamo una soluzione, puoi recedere dal servizio senza costi ed esportare i tuoi dati.

Il **manutentore che incarichi tu** non è un nostro sub-responsabile: è un soggetto che tu autorizzi ad accedere a una parte dei tuoi dati, e il rapporto con lui è tuo. Noi eseguiamo il tuo incarico e lo revochiamo quando lo revochi tu.

6. Quando ti aiutiamo

Diritti degli interessati. Se un tuo addetto o un tuo collaboratore esercita un diritto (accesso, rettifica, cancellazione, portabilità, limitazione, opposizione) rispondi tu. Il servizio ti mette in condizione di farlo da solo: i dati sono consultabili, modificabili, cancellabili ed esportabili dall'interfaccia — un addetto si corregge, si toglie dal servizio o si cancella senza lasciare traccia; una persona si toglie dagli accessi; il registro si esporta in PDF. Se non basta, ti assistiamo con misure tecniche adeguate. Se una richiesta arriva a noi, non rispondiamo nel merito e te la giriamo senza ritardo.

Violazioni dei dati. Se veniamo a conoscenza di una violazione che riguarda i tuoi dati, te lo comunichiamo **senza ingiustificato ritardo e comunque entro 48 ore** da quando ne siamo venuti a conoscenza, con: natura della violazione, categorie e numero approssimativo di interessati e di registrazioni, conseguenze probabili, misure adottate o proposte, e un recapito per avere altre informazioni. La notifica all'autorità e agli interessati, se dovuta, spetta a te: noi ti diamo ciò che ti serve per farla.

Valutazioni d'impatto. Ti assistiamo, per quanto ci riguarda e con le informazioni di cui disponiamo, in una valutazione d'impatto e nella consultazione preventiva (artt. 35 e 36).

7. Controlli e dimostrazione della conformità

Ti mettiamo a disposizione le informazioni necessarie a dimostrare il rispetto dell'art. 28, a partire da questo documento e dalla descrizione delle misure del punto 4.

Puoi svolgere una verifica **una volta l'anno** — o in qualunque momento dopo una violazione che ti riguarda — con trenta giorni di preavviso, in orario lavorativo, senza interferire con il servizio e nel

rispetto della riservatezza degli altri clienti: nessuna verifica può comportare l'accesso a dati di terzi o all'infrastruttura condivisa. I costi diretti di una verifica in loco sono a tuo carico, salvo che emerga una nostra inadempienza.

8. Alla fine del rapporto

Quando smetti di usare il servizio, **scegli tu**: restituzione o cancellazione dei dati. La cancellazione immediata la fai da solo, chiudendo l'organizzazione e scegliendo «cancella tutto, adesso»: il registro, le foto comprese, sparisce in quel momento. La restituzione avviene con l'esportazione del registro in PDF; se ti serve una copia completa in formato elaborabile, chiedila entro trenta giorni e te la forniamo.

In assenza di una tua indicazione diversa, cancelliamo i dati entro **dodici mesi** dalla chiusura. Le copie presenti nei backup si cancellano con la loro naturale rotazione (al più tardi dodici mesi), durante la quale restano protette dalle stesse misure e non vengono usate per nulla. Restano i documenti che dobbiamo conservare per obbligo di legge, come le fatture.

9. Varie

Se questo accordo e le condizioni di servizio dicono cose diverse sul trattamento dei dati personali, **vale questo accordo**. Si applica la legge italiana e, per quanto qui non previsto, il GDPR e il D.Lgs. 196/2003 come modificato.

Per ogni questione relativa a questo accordo: info@antincendio.it.

Sottoscrizione

Stampa, compila i dati mancanti e firma. Rimandaci una copia a info@antincendio.it: la controfirmiamo e te la restituiamo.

Il titolare del trattamento

Denominazione:

_____

P. IVA / C.F.:

_____

Sede:

_____

Rappresentante:

_____

Luogo e data:

_____

Firma

_____

Il responsabile del trattamento

Denominazione: Automa S.r.l.

P. IVA / C.F.: 16208401006

Sede: Via degli Olmetti 44/B int. C14, 00060 Formello (RM)

Rappresentante:

_____

Luogo e data:

_____

Firma

_____