



**ACaMIR**  
Agenzia Campana Mobilità Infrastrutture e Reti

# **MANUALE DI UTILIZZO DELLA PIATTAFORMA ACAMIR PER LE SEGNALAZIONI INTERNE (WHISTEBLOWING)**



## INDICE

Premessa .....	3
1. COLLEGAMENTO ALLA PIATTAFORMA DI SEGNALAZIONE .....	4
2. INSERIMENTO DI NUOVA SEGNALAZIONE .....	4
2.1. SEZIONE IDENTITÀ DEL SEGNALANTE .....	4
2.2. SEZIONE INFORMAZIONI PRELIMINARI .....	5
2.3. SEZIONE SEGNALAZIONE .....	5
2.4. SEZIONE ULTERIORI INFORMAZIONI .....	5
2.5. SEZIONE INFORMATIVA PRIVACY .....	5
2.6. SEZIONE INVIO DELLA SEGNALAZIONE .....	5
2.7. MODIFICHE DELLE SCHEDE .....	5
3. ACCEDERE ALLA SEGNALAZIONE GIÀ TRASMESSA.....	5

## Premessa

GlobaLeaks è una piattaforma informatica libera e open source conforme allo Standard ISO 37002, alla Direttiva EU 2019/1937, al Regolamento Generale sulla Protezione dei Dati (GDPR) nonché concessa in licenza con AGPLv3.0 e certificato OSI, per l'acquisizione e la gestione delle segnalazioni di fatti illeciti e delle comunicazioni di misure ritorsive, conformemente alle disposizioni di cui al D.lgs. 24/2023.

L'uso di GlobaLeaks su un Server Virtuale Privato (VPS) assicura, in conformità alle normative italiane ed europee sulla tutela dei *whistleblower*, che le informazioni siano gestite in modo confidenziale, crittografato e che l'identità dei segnalanti sia protetta, in linea con le disposizioni normative.

Per utilizzare la piattaforma assicurati che il dispositivo da te utilizzato soddisfi i seguenti requisiti tecnici:

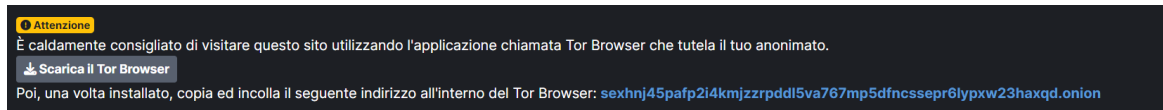
- Processore: dual-core da 2,0 GHz;
- RAM: 1GB;
- Archiviazione: 20 GB;
- I/O: 10Mbit/s (condiviso).

GlobaLeaks è progettato per funzionare su server anche più piccoli della configurazione di cui sopra. La dimensione dello spazio di archiviazione deve essere definita in base alle politiche di conservazione dei dati e all'utilizzo previsto della piattaforma.

La piattaforma è raggiungibile e fruibile attraverso un qualsiasi browser web (es. Firefox, Google, Safari) eseguiti su PC desktop, laptop, tablet e telefoni con sistemi operativi di Microsoft, IOS, Android.

### • Tor Browser

L'applicazione consiglia al segnalante, prima della compilazione della segnalazione, di installare sul dispositivo utilizzato il Tor Browser, tuttavia, per procedere alla segnalazione non è necessario installare tale browser.



Il Tor Browser protegge:

- l'anonimato degli utenti: mediante la navigazione anonima sul web non salvando la cronologia di navigazione e il tracciamento delle attività online, inclusi i nomi e gli indirizzi dei siti che visiti;
- la privacy e la sicurezza di rete.

Per maggiori informazioni sul browser consulta <https://tb-manual.torproject.org/it/about/>.

### • Key code

Si evidenzia che, inviata la segnalazione, la piattaforma genera un codice univoco crittografato di 16 cifre (cd. key code). Tale codice, non duplicabile e/o rigenerabile, può essere utilizzato per accedere alla piattaforma, controllare lo stato della segnalazione, aggiornare la propria segnalazione, inviare e ricevere comunicazioni e/o allegare eventuali altri documenti.

Si consiglia di conservare il codice in un luogo sicuro.

**ACaMIR - La tua segnalazione è andata a buon fine.**

Grazie. La tua segnalazione è andata a buon fine. Cercheremo di risponderti quanto prima.

Memorizza la tua ricevuta per la segnalazione.

3627 0866 5251 8276

Usa la ricevuta di 16 cifre per ritornare e vedere eventuali messaggi che ti avremo inviato o se pensi che ci sia altro che avresti dovuto allegare.

[Vedi la tua segnalazione](#)

### • Compilazione della segnalazione

I campi contrassegnati con l'asterisco (\*) sono obbligatori.

Nel caso di omessa selezione o descrizione delle informazioni richieste, la piattaforma non permette l'invio della segnalazione.

Cliccare il tasto "Successivo" per proseguire

Successivo

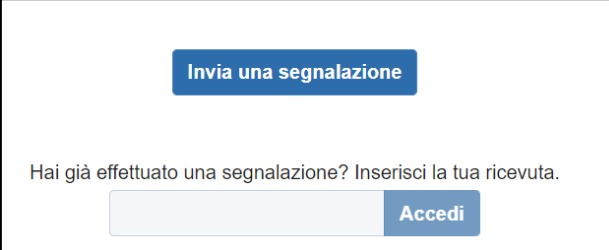
Precedente

È possibile allegare i documenti. A tal fine, si richiede che i documenti da allegare siano in formato .pdf non scansionati. Si consiglia di denominare gli stessi a seconda dell'oggetto.

## 1. COLLEGAMENTO ALLA PIATTAFORMA DI SEGNALAZIONE

Per accedere al software/piattaforma di segnalazione in qualità di soggetto segnalante (*whistleblower*) è necessario collegarsi alla pagina web: <https://acamir.regione.campania.it/segnalazioni-illeciti-whistleblowing/>.

Una volta collegati, si presenterà la seguente schermata.



Se si vuole presentare una nuova segnalazione  
(si veda p. 2 “Inserimento di una nuova segnalazione”)



cliccare il tasto “invia una segnalazione”

Se si vuole accedere ad una segnalazione già presentata  
(si veda p. 3 “Accedere ad una segnalazione già presentata”)



inserire il codice univoco di 16 cifre

## 2. INSERIMENTO DI NUOVA SEGNALAZIONE

Una volta cliccato il tasto “invia una segnalazione”, compariranno le seguenti schede:



Prima di iniziare la compilazione delle schede è necessario prendere visione del Regolamento recante la “Disciplina della procedura di gestione delle segnalazioni interne di condotte illecite (*Whistleblowing*)” dell’ACaMIR, approvato con Determinazione del Direttore Generale n. 488 del 24.10.2024.

Il regolamento è visionabile sul sito istituzionale dell’Agenzia al seguente indirizzo: <https://acamir.regione.campania.it/segnalazioni-illeciti-whistleblowing/>.

### 2.1. SEZIONE IDENTITÀ DEL SEGNALANTE

All’interno di questa sezione vengono richieste informazioni sul segnalante (*whistleblower*). In particolare, il segnalante può:

- scegliere se fornire i propri dati identificativi o rimanere anonimo;
- indicare, se ciò non comporta la propria identificazione, la qualifica e/o mansione o posizione professionale attuale;
- indicare, se ciò non comporta la propria identificazione, la denominazione della struttura, ente, società, organismo di diritto pubblico o del concessionario di pubblico servizio presso cui si presta servizio o attività;
- i contatti, qualora la piattaforma sia indisponibile.

**Attenzione:** Le segnalazioni effettuate in forma anonima saranno prese in considerazione solo se riguardano fatti di particolare gravità e siano adeguatamente circostanziate e rese con dovizia di particolari, tanto da far emergere fatti e situazioni specifici, relazionandoli a contesti determinati. Al di fuori di tale contesto, la segnalazione anonima è equiparata a segnalazione ordinaria e, pertanto, non configurandosi come una segnalazione di whistleblowing, non gode delle tutele previste dal d.lgs. n. 24/2023. Sarà comunque possibile dichiarare l’identità fino all’invio della segnalazione ovvero in un secondo momento accedendo alla piattaforma.

Nel caso in cui si forniscano i dati identificativi, tali dati saranno utilizzati e trattati secondo la normativa vigente in materia. In tal caso, l’identità del segnalante è protetta dalle tutele previste dal d. lgs. 24/2023.

Tutte le segnalazioni, nel rispetto della tutela della riservatezza dell’identità del segnalante, potranno essere inviate dal RPCT ad altre istituzioni (magistratura, Dipartimento della funzione pubblica, Corte dei conti, ecc.).

Se si forniscono i dati identificativi, si richiede al segnalante di acconsentire o non acconsentire alla rivelazione della identità qualora:

- nell’ambito di un procedimento disciplinare, la stessa sia indispensabile per la difesa dell’incolpato/a (Art. 12, comma 5, del D.Lgs. n. 24/2023);
- nelle procedure di segnalazione interna, la stessa sia indispensabile ai fini della difesa della persona coinvolta (Art. 12, comma 6, D.Lgs. n. 24/2023).

## 2.2. SEZIONE INFORMAZIONI PRELIMINARI

All'interno di questa sezione vengono richieste informazioni preliminari sul segnalante (*whistleblower*) sulla segnalazione. In particolare, viene richiesto:

- l'amministrazione/azienda/società partecipata, controllata/ in house dell'amministrazione a cui si riferisce la segnalazione;
- il rapporto intercorrente con l'amministrazione/azienda/società partecipata, controllata/ in house dell'amministrazione a cui si riferisce la segnalazione;
- se è stata già effettuata una segnalazione interna e se la stessa, ove rimasta inevasa, è stata sollecitata;
- se i fatti sono stati segnalati o denunciati a Procura, forze dell'ordine o ANAC le relative informazioni;
- se vi sono state discriminazioni o ritorsioni in seguito a segnalazioni interne o esterne già effettuate e, qualora subite, le relative informazioni.

## 2.3. SEZIONE SEGNALAZIONE

In tale sezione vengono richieste dettagliate informazioni relative ai fatti oggetto di segnalazione e le violazioni riscontrate (es. a titolo esemplificativo: conoscenza dei fatti, tipologia di condotta illecita, soggetti coinvolti, descrizione dei fatti, prove documentali, beneficiari dell'illecito, ecc.). Si raccomanda di rispondere ai quesiti nel modo più preciso ed esaustivo possibile.

**Attenzione:** La segnalazione deve essere circostanziata e avere ad oggetto fatti conosciuti e riscontrati direttamente dal segnalante. Le segnalazioni non adeguatamente circostanziate saranno suscettibili di richiesta di integrazioni da parte dell'RPCT, mediante il contatto indicato dal segnalante nella prima parte del modulo. Non sono considerate segnalazioni di whistleblowing quelle aventi ad oggetto una contestazione, rivendicazione o richiesta legata ad un interesse di carattere personale del segnalante.

## 2.4. SEZIONE ULTERIORI INFORMAZIONI

All'interno di questa sezione vengono richieste informazioni aggiuntive che possono aiutare il RPCT a gestire la segnalazione (es. a titolo esemplificativo: se si è già presentata una segnalazione ad uno o più enti/amministrazioni/società/aziende, coinvolti nella violazione, se i fatti segnalati sono oggetto di un contenzioso amministrativo, civile o contabile o un procedimento penale)

## 2.5. SEZIONE INFORMATIVA PRIVACY

In tale sezione si richiede al segnalante di:

- prendere visione dell'Informativa privacy – “Informazioni ai sensi dell'art. 13 del Regolamento (UE) 2016/679 - GDPR sul trattamento dei dati personali dei soggetti che segnalano fatti illeciti presso ACaMIR (whistleblowing) in base alle previsioni contenute nel decreto legislativo n. 24/2023” presente sul sito istituzionale dell'Ente al seguente indirizzo: <https://acamir.regione.campania.it/segnalazioni-illeciti-whistleblowing/>;
- di autorizzare il trattamento dei dati personali, laddove presenti nella segnalazione, per le finalità per cui la presente segnalazione è trasmessa al RPCT.

## 2.6. SEZIONE INVIO DELLA SEGNALAZIONE

Una volta compilate tutte le schede clicca “Invia” per inviare la segnalazione



Al momento dell'invio della segnalazione, la piattaforma genera un codice crittografato di 16 cifre (cd. key code). Tale codice, non duplicabile e/o rigenerabile, può essere utilizzato per accedere alla piattaforma, controllare lo stato della segnalazione, aggiornare la propria segnalazione, inviare e ricevere comunicazioni e/o allegare eventuali altri documenti.

## 2.7. MODIFICHE DELLE SCHEDE

Prima dell'invio della segnalazione, le schede possono sempre essere modificate, cliccando sul tasto “precedente” o, in alternativa, cliccando sulle singole schede.

## 3. ACCEDERE ALLA SEGNALAZIONE TRASMESSA

Per accedere alla segnalazione già presentata inserire il codice univoco di 16 cifre nell'apposito riquadro.

Invia una segnalazione

Hai già effettuato una segnalazione? Inserisci la tua ricevuta.

Accedi

Una volta inserito il codice è possibile visualizzare lo stato della segnalazione, il riepilogo del questionario e gli eventuali allegati inviati.

ID: 04fc8548-5411-40f8-a76d-81fcb961994			
🕒 Data	🕒 Ultimo aggiornamento	🗓 Scadenza	🟡 Stato
27-06-2024 14:24	27-06-2024 14:26	26-09-2024 02:00	Aperta
Risposte al questionario			▼
Allegati			▼
Commenti			▼

**Risposte al questionario:** In tale sezione il segnalante può visualizzare il riepilogo delle risposte inserite nella segnalazione trasmessa.

**Allegati:** In tale sezione il segnalante può visualizzare gli allegati inseriti nella segnalazione (non modificabili e non cancellabili) con la possibilità di allegare nuovi documenti ovvero integrare la documentazione caricando ulteriori file.

**Commenti:** In tale sezione il segnalante può visualizzare ogni aggiornamento relativo all’istruttoria, gestione e conclusione della segnalazione presentata, le richieste di integrazioni del RPCT nonché inserire ulteriori informazioni.

Commenti

0/4096

Invia

RPCT RICHIESTA DI INTEGRAZIONI	05-07-2024 12:08
RPCT RISCONTRO	05-07-2024 12:08
Whistleblower	27-06-2024 14:28

Per informazioni dettagliate sul software utilizzato, ivi comprese le misure di sicurezza tecniche ed i mezzi di crittografia adottati si rimanda alla documentazione GlobaLeaks: [docs.globaleaks.org/en/main/index.html](https://docs.globaleaks.org/en/main/index.html).

Per problemi relativi alla piattaforma ACaMIR per le segnalazioni interne “Globaleaks” contattare [m.palumbo@acamir.campania.it](mailto:m.palumbo@acamir.campania.it).