



**INFORMATIVA
AI SENSI DEL REGOLAMENTO GENERALE PER LA PROTEZIONE DEI DATI –
REGOLAMENTO UE 2016/679 E AL DECRETO LEGISLATIVO N. 196/2003 E
S.M.I. “CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI”**

PIATTAFORMA DI SEGNALAZIONE ILLECITI (WHISTLEBLOWING)

I dati personali forniti in fase di registrazione alla piattaforma per la segnalazione di illeciti (Whistleblowing) e nelle segnalazioni sono trattati in conformità al Regolamento Generale per la Protezione dei Dati - Regolamento UE 2016/679 e al Decreto Legislativo n. 196/2003 e s.m.i. “Codice in materia di protezione dei dati personali” come novellato dal D. Lgs. 101/2018 e nel rispetto degli obblighi di riservatezza imposti dalla normativa sulla privacy, dal D. Lgs. 10 marzo 2023, n. 24 “Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001”.

La presente informativa è resa ai sensi Regolamento Generale per la Protezione dei Dati – Regolamento UE 2016/679.

1. Titolare del Trattamento, Responsabile della protezione dei dati

Il Titolare del Trattamento è l'Università degli Studi dell'Insubria, nella persona del Magnifico Rettore, con sede legale in Varese (VA) Via Ravasi, 2, pec ateneo@pec.uninsubria.it.

Gli Interessati possono rivolgersi al Responsabile della protezione dei dati per l'esercizio dei diritti previsti dal GDPR (artt. da 12 a 21) utilizzando il seguente indirizzo e-mail: privacy@uninsubria.it. L'elenco aggiornato dei responsabili e degli autorizzati al trattamento è custodito presso la sede del Titolare del trattamento.

2. Oggetto del trattamento

- Dati comuni forniti dall'interessato in fase di registrazione: Nome, eventuale secondo nome, Cognome, data di nascita, indirizzo mail, scansione di un documento di identità in corso di validità.
- In caso di accesso/registrazione mediante identità SPID: i dati personali restituiti da SPID alla piattaforma: Nome, Cognome, Codice Fiscale, spidCode, Luogo di Nascita, Data di nascita, Genere, Numero del documento di identità, numero di telefono cellulare, indirizzo mail privato, indirizzo di residenza; Nota: i dati personali, relativi al profilo di accesso alla piattaforma, oggetto di cifratura, non sono direttamente visualizzabili nella segnalazione effettuata.
- Dati personali di soggetti relativi alla segnalazione;
- Contenuto della segnalazione;
- Per gli operatori abilitati a operare sul sistema, RPCT e gruppo di supporto, dati relativi alle attività svolte sulla piattaforma;



- *Cookies*:
 - Nessun dato personale degli utenti viene implicitamente acquisito dalla piattaforma.
 - Non viene fatto uso di cookies per la trasmissione di informazioni di carattere personale, né vengono utilizzati *cookies* persistenti per il tracciamento degli utenti.
 - Vengono utilizzati esclusivamente *cookies* tecnici nella misura strettamente necessaria al corretto ed efficiente utilizzo della piattaforma. L'uso dei *cookies* di sessione (che non vengono memorizzati in modo persistente sul computer dell'utente e svaniscono con la chiusura del *browser*) è strettamente limitato alla trasmissione di identificativi di sessione (costituiti da numeri casuali generati dal server) necessari per consentire l'esplorazione sicura ed efficiente della piattaforma;
- Per quanto riguarda i log relativi alle attività di navigazione effettuate da dispositivi collegati alla rete di Ateneo, è stata implementata una specifica regola sui firewall per mezzo della quale è stata esclusa la registrazione nei log delle attività di accesso verso la piattaforma per la segnalazione di illeciti.

3. Finalità del trattamento cui sono destinati i dati:

I dati forniti saranno oggetto di trattamento, in relazione agli obblighi di cui al D. Lgs. 10 marzo 2023, n. 24 “Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001”.

Non sono previsti ulteriori trattamenti basati sui legittimi interessi perseguiti dal Titolare del trattamento.

4. Base Giuridica dei Trattamenti

La base giuridica del trattamento, ai sensi degli artt. 6, comma 1, lettera c) e e), 9, comma 2, lettera g), e 10 del GDPR – nonché artt. 2 ter e sexies del D.Lgs. 196/2003, è la necessità di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento nonché di adempiere a un obbligo legale al quale è soggetto il titolare del trattamento.

5. Obbligatorietà o meno del conferimento dei dati

Tenuto conto delle finalità del trattamento sopra illustrate, il conferimento dei Suoi dati di registrazione (nominativo, indirizzo e-mail e documento di riconoscimento) è obbligatorio ed il loro mancato conferimento ha come conseguenza l'impossibilità di creare un *whistleblower* (soggetto segnalante) riconoscibile nel sistema.

Si ricorda che la normativa, prevede che il *whistleblower* si renda riconoscibile al fine di potersi avvalere del regime di tutela accordatogli.

Il trattamento dei dati personali del soggetto segnalato o di eventuali soggetti coinvolti nella segnalazione è lecito anche senza il consenso degli interessati, in quanto necessario al perseguimento di motivi di interesse pubblico rilevante.

6. Modalità del trattamento

Il trattamento sarà effettuato con strumenti informatici e telematici con logiche di organizzazione ed elaborazione strettamente correlate alle finalità sopra indicate e comunque in modo da garantire

la sicurezza, l'integrità e la riservatezza dei dati stessi nel rispetto delle misure organizzative, fisiche e logiche previste dalle disposizioni vigenti. Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati nel pieno rispetto dell'art. 32 del GDPR.

Si ricorda che i Suoi dati personali forniti nel *form* di registrazione (nominativo, indirizzo e-mail e documento di riconoscimento) sono separati dalle segnalazioni e che l'associazione della Sua identità con la segnalazione può essere effettuata esclusivamente dal “*Responsabile della Prevenzione della Corruzione e della Trasparenza*” - RPCT preposto alla gestione delle segnalazioni, nel caso in cui lo ritenga necessario ai fini dell'accertamento della fondatezza della segnalazione. Tale azione viene automaticamente notificata al segnalante (unitamente alla motivazione a fondamento della richiesta del RPCT) e registrata nel sistema.

7. Periodo di conservazione dei dati

I dati personali relativi alle segnalazioni vengono conservati e mantenuti per tutto il tempo necessario in adempimento alla procedura di gestione delle segnalazioni di illeciti in conformità a quanto previsto dall'art.14 del D. Lgs. n. 24/2023 e conservati agli atti.

In particolare, le segnalazioni interne e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del D.lgs. n. 24/2023 e del principio di cui agli articoli 5, paragrafo 1, lettera e), del regolamento (UE) 2016/679 e 3, comma 1, lettera e), del decreto legislativo n. 51 del 2018.

In particolare, si procede alla:

1. distruzione o anonimizzazione immediata dei dati personali relativi ad una segnalazione giudicata non rientrante nel perimetro del sistema di whistleblowing implementato;
2. distruzione o anonimizzazione entro due mesi dal compimento delle operazioni di verifica in ordine ai fatti segnalati, ove tali operazioni non abbiano avuto ulteriore seguito, nell'ipotesi di dati personali relativi ad una segnalazione giudicata rientrante nel perimetro del sistema di whistleblowing implementato;
3. conservazione fino alla conclusione del procedimento e allo spirare dei termini di impugnazione per come previsti dalla legislazione nazionale di riferimento, nel caso in cui alla segnalazione abbia fatto seguito un'azione giudiziaria o disciplinare nei confronti del soggetto segnalato o segnalante.

8. Soggetti o categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di Responsabili o Autorizzati

I dati trattati per le finalità di cui sopra potranno essere comunicati o potranno essere accessibili ai dipendenti assegnati al personale degli uffici dell'Università degli Studi dell'Insubria che, con specifico atto, è incaricato di operare quale supporto del “*Responsabile della Prevenzione della Corruzione e della Trasparenza*” - RPCT, soggetti autorizzati dal Titolare (art. 29 GDPR 2016/679).

Sono destinatari dei dati raccolti a seguito della segnalazione, se del caso, l'Autorità Giudiziaria, la Corte dei conti e l'ANAC.

La gestione e la conservazione dei dati personali raccolti avviene presso il datacenter del fornitore della piattaforma, nominato quale Responsabile del trattamento a norma dell'art. 28 del GDPR.

L'elenco completo ed aggiornato dei Responsabili del trattamento è conoscibile a mera richiesta presso la sede del titolare.



9. Trasferimento dati all'estero

I dati collegati sono raccolti e mantenuti presso il datacenter del fornitore presente sul territorio italiano.

10. Diritti dell'Interessato

Questi sono i diritti esercitabili nei confronti dell'Università degli Studi dell'Insubria (Titolare del trattamento):

- diritto di accesso ai propri dati personali ed a tutte le informazioni di cui all'art.15 del GDPR,
- diritto di rettifica dei propri dati personali inesatti e l'integrazione di quelli incompleti,
- diritto di cancellazione dei propri dati, fatta eccezione per quelli contenuti in atti che devono essere obbligatoriamente conservati dall'Università e salvo che sussista un motivo legittimo prevalente per procedere al trattamento;
- diritto alla limitazione del trattamento ove ricorra una delle ipotesi di cui all'art. 18 del GDPR.
- diritto di opporsi al trattamento dei propri dati personali, fermo quanto previsto con riguardo alla necessità ed obbligatorietà del trattamento ai fini dell'instaurazione del rapporto
- diritto di revocare il consenso eventualmente prestato per i trattamenti non obbligatori dei dati, senza con ciò pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca.

Si segnala che ai sensi dell'art.2- undecies, lett. f) del D.Lgs. 196/2003 i diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del GDPR qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità della persona che segnala violazioni di cui sia venuta a conoscenza in ragione del proprio rapporto di lavoro o delle funzioni svolte, ai sensi del decreto legislativo recante attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione, ovvero che segnala violazioni ai sensi degli articoli 52-bis e 52-ter del decreto legislativo 1° settembre 1993, n. 385, o degli articoli 4-undecies e 4-duodecies del decreto legislativo 24 febbraio 1998, n. 58.

Per l'esercizio di questi diritti l'Interessato può rivolgersi al Responsabile della protezione dei dati inviando la richiesta via mail all'indirizzo privacy@uninsubria.it.

11. Reclamo

L'Interessato ha inoltre diritto di avanzare un reclamo al Garante per la Protezione dei Dati Personali (www.garanteprivacy.it) o all'Autorità Garante dello Stato dell'UE in cui l'Interessato risiede abitualmente o lavora, oppure del luogo ove si è verificata la presunta violazione, in relazione a un trattamento che consideri non conforme.