

**SEGNALAZIONI DI VIOLAZIONI DEL DIRITTO NAZIONALE E DELL'UNIONE EUROPEA  
(WHISTLEBLOWING). INFORMAZIONI AI SENSI DEGLI ARTICOLI 13 E 14 DEL REGOLAMENTO (UE)  
2016/679, REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI PERSONALI (GDPR)**

Si forniscono con la presente le informazioni previste dagli articoli 13 e 14 del GDPR in relazione al trattamento dei dati personali che viene posto in essere nell'ambito del cd. "*whistleblowing*", ossia la segnalazione di violazioni di disposizioni normative nazionali o dell'Unione Europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica di cui il segnalante sia venuto a conoscenza nel proprio contesto lavorativo.

**TITOLARE DEL TRATTAMENTO, RESPONSABILE DELLA PROTEZIONE DEI DATI E RELATIVI DATI DI CONTATTO**

Titolare del trattamento è l'Azienda Ospedaliera Universitaria Integrata Verona (AOUI Verona), con sede in Piazzale Stefani, 1, 37126 Verona; i relativi dati di contatto sono reperibili sulla home page del sito istituzionale di AOUI Verona raggiungibile all'indirizzo [www.aovr.veneto.it](http://www.aovr.veneto.it).

Il responsabile aziendale della protezione dei dati può essere contattato inviando una e-mail all'indirizzo: [rpd@aovr.veneto.it](mailto:rpd@aovr.veneto.it).

**CATEGORIE DI DATI PERSONALI TRATTATI**

Sono oggetto di trattamento i dati personali forniti dal segnalante al fine di rappresentare le presunte violazioni di disposizioni normative nazionali o dell'Unione Europea che ledono l'interesse pubblico o l'integrità di AOUI Verona, di cui il segnalante sia venuto a conoscenza nel contesto lavorativo.

In particolare, la ricezione e la gestione delle segnalazioni può dar luogo, a seconda del contenuto delle segnalazioni e degli atti e documenti a queste allegati, al trattamento di:

- dati personali c.d. "comuni" (ad es., dati anagrafici, dati di contatto, ruolo professionale);
- dati personali c.d. "particolari" (ad es., dati relativi alla salute, all'appartenenza sindacale, e altri di cui all'art. 9 del GDPR);
- dati personali c.d. "giudiziari", relativi a condanne penali, reati e connesse misure di sicurezza di cui all'art. 10 del GDPR.

I dati personali si riferiscono al soggetto segnalante e possono altresì riferirsi a persone indicate come possibili responsabili delle condotte illecite, nonché a quelle a vario titolo coinvolte nelle vicende segnalate.

Ai sensi dell'art. 13, comma 2, del d.lgs. 10/03/2023, n. 24, che ha dato attuazione alla direttiva UE 2019/1937 sulla protezione delle persone che segnalano violazioni del diritto dell'Unione e delle disposizioni normative nazionali, i dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.

**FINALITÀ DEL TRATTAMENTO E RELATIVA BASE GIURIDICA**

I dati personali sono trattati unicamente per la gestione della segnalazione della violazione e per gli adempimenti conseguenti (eventuali comunicazioni alle competenti Autorità, eventuale attivazione di procedimento disciplinare nei confronti del segnalato, etc.), ove essa sia ritenuta fondata all'esito dell'istruttoria condotta dal Responsabile della prevenzione della corruzione e della trasparenza (RPCT), con l'eventuale ausilio della sua struttura di supporto.

Quanto alla base giuridica, il trattamento dei dati personali è necessario per l'adempimento di un obbligo legale cui è soggetto il titolare del trattamento (art. 6, par. 1, lett. c), GDPR in relazione al d.lgs. 24/2023).

In linea di principio, il consenso dell'interessato (art. 6, par. 1, lett. a), GDPR) non è una base giuridica del trattamento; lo diventa quando vi è la necessità di rivelare l'identità del segnalante a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, in particolare, nel procedimento disciplinare, laddove il disvelamento dell'identità del segnalante sia indispensabile per la difesa del soggetto a cui viene contestato l'addebito disciplinare, e nei procedimenti instaurati in seguito alla segnalazione, laddove tale rivelazione sia indispensabile anche ai fini della difesa della persona coinvolta (vedasi anche il successivo paragrafo sui DIRITTI DEGLI INTERESSATI).

Con riguardo al trattamento di categorie particolari di dati, l'eccezione al divieto di trattarli può essere rinvenuta nella necessità di assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento e dell'interessato in materia di diritto del lavoro (art. 9, par. 2, lett. b), GDPR), nonché per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri (art. 9, par. 2, lett. g), GDPR, in relazione: a) al d.lgs. 24/2023, che ha recepito la direttiva UE 2019/1937; b) all'art. 2-sexies, comma 2, lett. dd), del d.lgs. 30/06/2003, n. 196, Codice in materia di protezione dei dati personali).

Infine, i dati personali relativi a condanne penali e reati possono essere trattati ai sensi dell'art. 10 del GDPR perché il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri (d.lgs. 24/2023, che ha recepito la direttiva UE 2019/1937; art. 2-octies del d.lgs. 196/2003).

### **CATEGORIE DI DESTINATARI DEI DATI**

L'analisi e la preliminare verifica sulla fondatezza delle circostanze rappresentate nella segnalazione sono affidate al RPCT che vi provvede nel rispetto dei principi di imparzialità e riservatezza effettuando ogni attività ritenuta opportuna, inclusa l'audizione personale del segnalante, della persona coinvolta e di eventuali altri soggetti che possono riferire sui fatti segnalati. Qualora, all'esito della verifica, si ravvisino elementi di non manifesta infondatezza del fatto segnalato, il Responsabile provvederà a trasmettere l'esito dell'accertamento:

- agli organi e alle strutture competenti di AOUI Verona affinché adottino gli eventuali provvedimenti e/o le azioni ritenuti necessari, anche a tutela dell'Azienda stessa;
- se del caso, alle Autorità competenti (ad es., Corte dei conti, Giudice penale), sempre tutelando la riservatezza del segnalante.

Qualora il RPCT debba avvalersi di personale aziendale di supporto ai fini della gestione delle segnalazioni, tale personale è appositamente autorizzato al trattamento dei dati personali e, di conseguenza, dovrà attenersi al rispetto delle istruzioni impartite, nonché di quelle più specifiche, connesse al particolare trattamento, di volta in volta fornite dal RPCT.

Se per ragioni istruttorie anche altri soggetti debbano essere messi a conoscenza del contenuto della segnalazione e/o della documentazione ad essa allegata, il trattamento di tali elementi sarà improntato alla massima cautela, a cominciare dall'oscuramento dei dati personali relativi al segnalante e agli altri soggetti la cui identità in base al d.lgs. 24/2023 deve rimanere riservata.

Infine, è stata nominata responsabile del trattamento ai sensi dell'art. 28 del GDPR la ditta Whistleblowing Solutions I.S. S.r.l. di Milano, la cui piattaforma digitale di *whistleblowing* è utilizzata per le segnalazioni.

### **PERIODO DI CONSERVAZIONE DEI DATI**

I dati acquisiti in conseguenza delle segnalazioni verranno conservati in una forma che consenta l'identificazione degli interessati per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data di comunicazione dell'esito finale della procedura di segnalazione, salva la necessità di conservarli per un tempo più lungo per motivate esigenze legate a procedimenti ancora pendenti in ambito penale, civile, contabile o disciplinare.

Il gestore della piattaforma garantisce in ogni caso la cancellazione automatica sicura dei dati caricati a sistema dopo dodici mesi dalla data della segnalazione, salva la possibilità per il titolare del trattamento di anticipare o posticipare tale termine secondo le necessità contingenti.

## **DIRITTI DEGLI INTERESSATI**

Ai sensi del d.lgs. 24/2023, l'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate, senza il consenso espresso della stessa, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni. In più, in due casi particolari, per rivelare l'identità del segnalante, oltre al consenso espresso dello stesso, si richiede anche una comunicazione scritta a costui delle ragioni di tale rivelazione:

- nel procedimento disciplinare conseguente alla segnalazione, laddove il disvelamento dell'identità del segnalante sia indispensabile per la difesa del soggetto a cui viene contestato l'addebito disciplinare;
- in altri procedimenti instaurati in seguito alla segnalazione, laddove tale rivelazione sia indispensabile anche ai fini della difesa della persona coinvolta.

Alla segnalazione e all'identità del segnalante non è possibile accedere né a mezzo accesso documentale, né a mezzo accesso civico generalizzato.

La tutela dell'identità viene garantita anche alla persona coinvolta e alle persone menzionate nella segnalazione fino alla conclusione dei procedimenti avviati in ragione della segnalazione stessa, nel rispetto delle medesime garanzie previste in favore della persona segnalante, salvo il caso in cui la segnalazione sia oggetto di denuncia alle Autorità giudiziarie.

La violazione dell'obbligo di riservatezza da parte di chi è incaricato di ricevere o dare seguito alle segnalazioni è fonte di responsabilità disciplinare, fatte salve ulteriori forme di responsabilità previste dall'ordinamento.

Accanto al diritto alla tutela della propria identità, sono altresì garantiti agli interessati i diritti previsti dalla normativa sulla protezione dei dati personali, ossia:

- il diritto di accesso ai propri dati personali e ad altre informazioni, una volta ottenuto conferma dal titolare del trattamento che è in corso un trattamento di dati personali che li riguardano (art. 15 GDPR);
- il diritto di rettifica dei dati personali inesatti che li riguardano, e di integrazione di quelli incompleti (art. 16 GDPR);
- il diritto di limitazione del trattamento dei dati personali che li riguardano, ricorrendone le condizioni stabilite dalla vigente normativa (art. 18 GDPR);
- nei limitati casi in cui il trattamento è basato sul consenso dell'interessato (vedi *supra*), il diritto di revocare tale consenso in qualsiasi momento, fermo restando che la revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca.

L'apposita istanza va rivolta al Responsabile della prevenzione della corruzione e della trasparenza all'indirizzo [segnalazioneilleciti@aovr.veneto.it](mailto:segnalazioneilleciti@aovr.veneto.it). Gli interessati possono anche contattare il responsabile aziendale della protezione dei dati all'indirizzo di posta elettronica indicato sopra.

Gli interessati i quali ritengono che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dal GDPR hanno il diritto di proporre reclamo al Garante per la protezione dei dati personali (informazioni al riguardo si possono rinvenire sul sito [www.garanteprivacy.it](http://www.garanteprivacy.it)), come previsto dall'art. 77 del Regolamento stesso.

Peraltro, i diritti di cui sopra non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo al Garante per la protezione dei dati personali, qualora dall'esercizio di tali diritti possa derivare

un pregiudizio effettivo e concreto alla riservatezza dell'identità del segnalante. L'esercizio dei medesimi diritti può, in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare l'interesse del segnalante alla tutela della propria riservatezza. Resta ferma la possibilità per l'interessato di esercitare i propri diritti con le modalità previste dall'art. 160 del d.lgs. 196/2003, che prevede particolari accertamenti da parte del Garante per la protezione dei dati personali, il quale informa l'interessato di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto di proporre ricorso giurisdizionale (art. 2-undecies, d.lgs. 196/2003).

#### **OBBLIGO DI CONFERIMENTO DEI DATI PERSONALI E FONTE DA CUI I DATI PERSONALI HANNO ORIGINE**

Per il segnalante la comunicazione dei dati personali è funzionale alla segnalazione, e dunque, in caso di mancato conferimento dei dati, la segnalazione segue la sorte delle segnalazioni anonime, ossia vengono prese in considerazione se adeguatamente circostanziate, ma non attivano le protezioni riconosciute al *whistleblower*. La segnalazione è la fonte da cui hanno origine i dati personali della persona coinvolta e delle eventuali altre persone menzionate nella stessa.