# Registro del trattamento: Gestione sistema Whistleblowing

Il soggetto giuridico Istituti Riuniti Salotto e Fiorito i cui recapiti sono

Rif.GDPR art.30(1.a),(2.a)

Indirizzo: Via Grandi 5 RIVOLI 10098 (TO)

email: e-mail direzione@salfior.it;

PEC Istituto paritario: [istruzione@pec.salfior.it](mailto:istruzione@pec.salfior.it);

PEC Agenzia Formazione: formazione@pec.salfior.it

tel.: 011.956.17.15

web: [https://formazione.salottoefiorito.it](https://urlsand.esvalabs.com/?u=https%3A%2F%2Fformazione.salottoefiorito.it%2F&e=2c48af4b&h=acd3458d&f=y&p=y)

agisce in qualità di

**- Titolare**

**Il trattamento riguarda**:

L'attività di trattamento riguarda l'implementazione del sistema di segnalazione e la gestione delle segnalazioni di violazioni (del diritto europeo e/o nazionale) che ledono l’interesse pubblico o l’integrità dell’Amministrazione pubblica o dell’ente privato, di cui il soggetto segnalante sia venuto a conoscenza in ragione del proprio rapporto di servizio con la scrivente organizzazione, compreso:

- la gestione e preliminare verifica sulla fondatezza delle circostanze rappresentate nella segnalazione

- l’audizione personale del segnalante e di eventuali altri soggetti che possono riferire sui fatti segnalati

- gli approfondimenti istruttori o per l’adozione dei provvedimenti

- comunicazione di misure ritorsive

**Finalità**: Rif.GDPR art.30(1.b),(2.b)

- Adempimento di un obbligo legale al quale è soggetto l'ente (in ottemperanza al D.Lgs. 24/2023, che recepisce la direttiva UE 2019/1937, riguardante la protezione delle persone che segnalano violazioni del diritto dell’Unione Europea)

- Adempimento di un obbligo legale al quale è soggetto l'ente (nei casi di adozione del Modello Organizzativo ex art. 6 del d.lgs. 231/2001 per la prevenzione della responsabilità amministrativa da reato)

- Prevenire e contrastare le condotte illegali all’interno della scrivente organizzazione

- Effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l’adozione dei conseguenti provvedimenti

**Interessati**: Rif.GDPR art.30(1.c),(2.b)

- soggetti segnalanti (azionisti, dirigenti, amministratori, dipendenti, fornitori, consulenti, tirocinanti, lavoratori autonomi,)

- dipendenti di altre amministrazioni in posizione di comando, distacco o fuori ruolo presso la scrivente organizzazione

- facilitatori (persona fisica che assiste una persona segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata)

- persone nei confronti delle quali sono state effettuate delle segnalazioni che le riguardano

- terzi identificati e identificabili (aventi causa con i soggetti segnalanti e/o persone coinvolte nelle segnalazioni)

**Tipi di dati**: Rif.GDPR art.30(1.c),(2.b)

- personali

- relativi a comportamenti illeciti o fraudolenti

- dati personali, potenzialmente anche appartenenti a categorie particolari, forniti dal segnalante al fine di rappresentare le presunte condotte illecite

- potenzialmente anche dati particolari (corruzione medica es. <https://www.libertasicilia.it/siracusa-corruzione-nella-sanita-soldi-in-cambio-di-false-certificazioni-mediche-indagato-dirigente-medico-dellasp-aretusea/> o del medico del lavoro, magari per dichiarare l’inabilità di un lavoratore sgradito)

**Categorie di Destinatari** (oltre alle persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile del trattamento): Rif.GDPR art.30(1.d)

- Gestore delle segnalazioni

- Fornitore del servizio di erogazione e gestione operativa del canale di segnalazione interno

- Fornitore del servizio di erogazione e gestione operativa del canale di segnalazione esterno

- Autorità Nazionale Anticorruzione

- Autorità giudiziarie

**Trasferimenti extra UE**: Rif.GDPR art.30(1.e),(2.c)

Non sono previsti trasferimenti verso paesi terzi ovvero organizzazioni internazionali.

**Termini ultimi previsti per la cancellazione**: Rif.GDPR art.30(1.f)

I dati di ogni categoria sono conservati:

- I dati personali, le segnalazioni e la relativa documentazione saranno conservati in generale, fintanto che perdurano le finalità del trattamento e per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque (5) 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 decreto legislativo n. 24 del 2023.

- decorso il termine di conservazione, si procede periodicamente alla cancellazione non automatica.

**Misure di sicurezza tecniche e organizzative**: Rif.GDPR art.30(1.g),(2.d)

Oltre a quanto indicato nel paragrafo “Misure generali”, e in quello “Misure relative alle sedi”, a livello specifico del trattamento, vanno considerate le seguenti misure, prevalentemente tecniche:

- minimizzazione dei dati personali trattati.

- profili di autorizzazione specifici, diversificati per ciascun utente.

- adozione del Regolamento Whistleblowing per l’implementazione del sistema di segnalazione interno e la gestione delle segnalazioni ricevute.

- strumenti di crittografia (a garanzia della riservatezza dell’identità della persona segnalante, della persona coinvolta, nonché del contenuto della segnalazione e della relativa documentazione).

- Nell'ambito del procedimento disciplinare, sussiste il divieto di rilevare l'identità della persona segnalante ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa.

\* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~ \* ~

**Presupposti di legittimità**:

- Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (in ottemperanza al D.Lgs. 24/2023, che recepisce la direttiva UE 2019/1937, riguardante la protezione delle persone che segnalano violazioni del diritto dell’Unione Europea).

- Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (nei casi di adozione del Modello Organizzativo ex art. 6 del d.lgs. 231/2001 per la prevenzione della responsabilità amministrativa da reato).

- Il trattamento è necessario per l'esecuzione di un compito di interesse pubblico (con particolare riferimento a quanto disposto dall’articolo 1, comma 1 e articolo 2, comma 1 del d.lgs. 24/2023 e della Direttiva 2019/1937, e al compito di accertare eventuali illeciti denunciati nell’interesse dell’integrità dell’Ente, ai sensi dell’art. 54-bis del d.lgs. n. 165/2001).

- L'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità (in via residuale qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell’identità del segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione potrà essere utilizzata ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità).

**Modalità di raccolta dei dati degli interessati**:

**Diffusione dei dati**:

Le modalità utilizzate sono:

- In casi eccezionali, nei casi e con le modalità specificate al D.Lgs. 24/2023, è prevista la possibilità di effettuare la segnalazione mediante la divulgazione pubblica attraverso i media.

**Soggetti coinvolti, nell’ambito del trattamento consentito**:

- Riferimento interno

- Gestore delle segnalazioni

- Fornitore del servizio di erogazione e gestione operativa del canale di segnalazione interno

- Fornitore del servizio di erogazione e gestione operativa del canale di segnalazione esterno (Anac - Autorità Nazionale Anticorruzione)

- Organi di Controllo della scrivente organizzazione (es. collegio sindacale, ODV, DPO, auditor interni o esterni) (per approfondimenti istruttori o per l’adozione dei provvedimenti)

- Autorità giudiziarie

**Ulteriori informazioni**:

Il trattamento non è occasionale.

Il trattamento non rientra tra quelli propri e specifici delle attività principali svolte.

Il trattamento non va considerato su larga scala, tenuto conto di: il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; la durata, ovvero la persistenza, dell’attività di trattamento; la portata geografica dell’attività di trattamento.

Il trattamento non utilizza nuove tecnologie della società dell’informazione.

**Asset specifici e non generici sono utilizzati per il trattamento in questione**:

- Dispositivo Strumenti hardware e applicativi di uso comune (personal PC, stampante multifunzione, fogli di testo, fogli di calcolo, internet, e-mail, etc..)

- Servizio Canale di segnalazione interno come indicato al Regolamento whistleblowing

- Servizio Canale di segnalazione esterno <https://whistleblowing.anticorruzione.it>

**Valutazione dei rischi**:

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché delle misure tecniche e organizzative messe in atto, il trattamento non è rischioso per i diritti e le libertà delle persone fisiche: in particolare il rischio generale residuo è da considerarsi:

- Accettabile

**Adempimenti eventualmente conseguenti**:

* La valutazione di impatto risulta necessaria e/o obbligatoria.
* La designazione del Data Protection Officer (DPO), quale Responsabile della protezione dei dati non risulta necessaria e/o obbligatoria.
* In uno scenario generico di avvenuta violazione dei dati (Data-Breach), considerando:

- la natura, l'ambito di applicazione, il contesto, le finalità del trattamento, le categorie di interessati, i dati personali trattati e,

- i rischi potenziali per le libertà e i diritti fondamentali delle persone fisiche interessate dal trattamento;

è da ritenersi **sempre obbligatorio:**

- registrare l’evento nel Registro delle Violazioni dei dati (RVD);

Ciò non di meno occorre svolgere la **valutazione di impatto della violazione specifica caso per caso, secondo procedura**, in particolare:

- in caso di incidenti di sicurezza, qualora dalla valutazione, i rischi individuati risultino non trascurabili per le persone fisiche, il Titolare del trattamento deve notificare la violazione all’Autorità di Controllo entro 72 ore dalla scoperta;

- nei casi in cui la valutazione abbia rilevato dei rischi elevati per le persone fisiche, il Titolare del trattamento deve comunicare a tutti gli interessati coinvolti l’avvenuta violazione con le indicazioni per ridurre i rischi a loro carico;