



Whistleblowing e protezione dei dati personali nei Comuni

A domanda risponde Prof. Avv. Michele IASELLI

14 Gennaio 2024 - dalle ore 11.30 alle 12.30

ASMEL - Associazione per la Sussidiarietà e la Modernizzazione degli Enti Locali

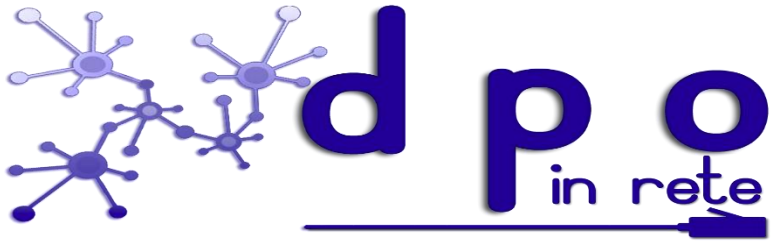
Email info@dpointrete.it

Numero Verde 800.16.56.54

Web: www.dpointrete.it

www.asmel.eu



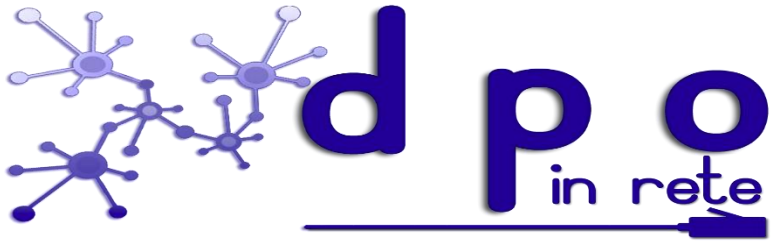


Cos'è il whistleblowing

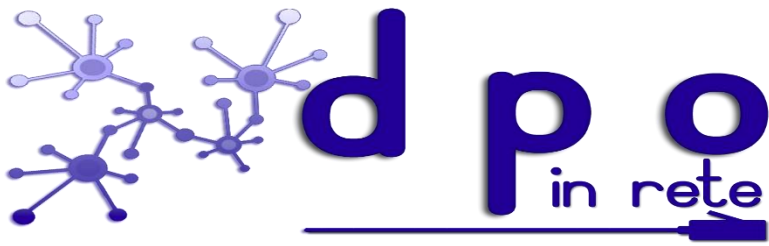


Il whistleblowing è un termine anglosassone che si riferisce alla segnalazione di illeciti, irregolarità o comportamenti non conformi all'interno di un'organizzazione da parte di dipendenti, collaboratori o soggetti che ne sono venuti a conoscenza.

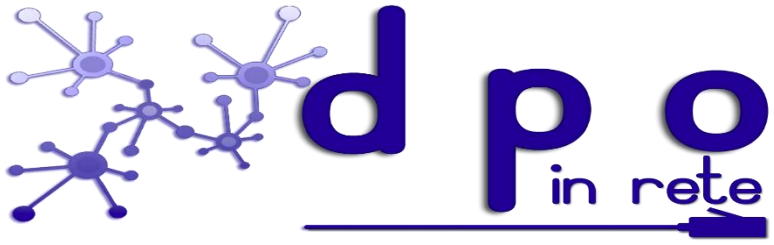
La figura del whistleblower è la persona che denuncia tali comportamenti, generalmente rivolti alla violazione di leggi o regolamenti, alla corruzione, frode o altri comportamenti illeciti.



Normativa applicabile



Il Decreto Legislativo n. 24 del 10 marzo 2023 disciplina il whistleblowing in Italia. Questo decreto recepisce la Direttiva (UE) 2019/1937 sulla protezione delle persone che segnalano violazioni del diritto dell'Unione (la cosiddetta "Direttiva Whistleblowing").



Principali aspetti del D.lgs. n. 24/2023



Ambito di applicazione

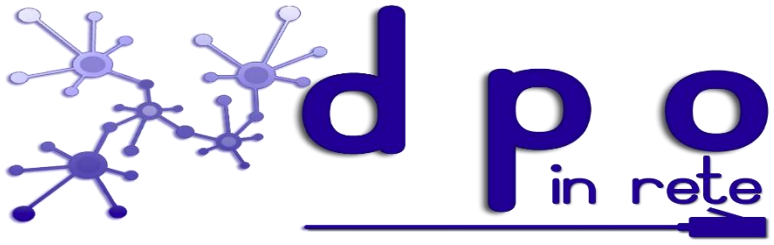
Canali di segnalazione

Protezione del whistleblower

Violazioni che possono essere segnalate

Sanzioni

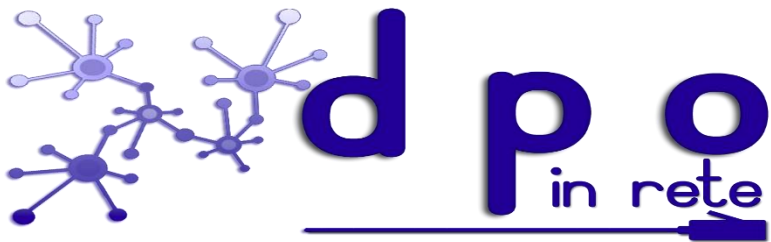
Figure protette



Protezione dei dati e segnalazioni di irregolarità



La protezione dei dati personali nel contesto delle segnalazioni di irregolarità è regolata principalmente dal D.lgs. n. 24/2023 e dal Regolamento (UE) 2016/679 (GDPR). Questa disciplina si concentra su diversi aspetti per garantire che il trattamento dei dati sia conforme alla normativa, rispettando i diritti degli interessati e favorendo un sistema di segnalazione sicuro ed efficace.



Principi fondamentali del trattamento dei dati

Protezione dell'identità del segnalante

Trattamento dei dati del segnalato

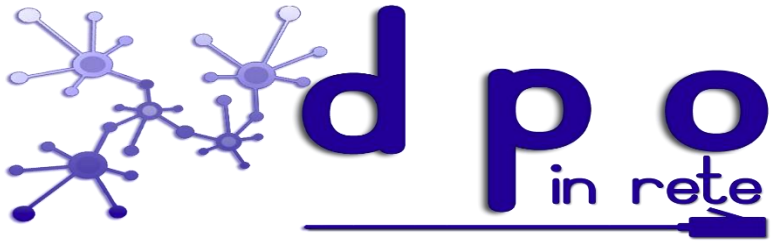
Conservazione dei dati

Misure tecniche ed organizzative

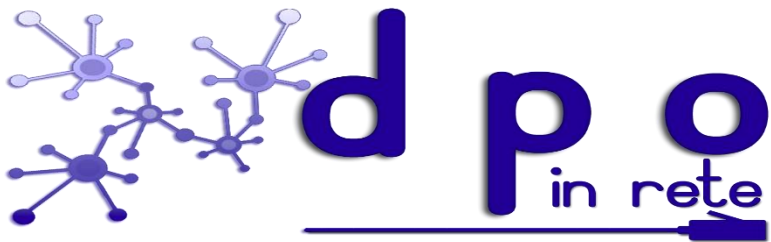
DPIA

Ruolo del DPO

Diritti degli interessati



Attuazione di un sistema di segnalazione nei Comuni



Requisiti per l'implementazione del sistema

Scelta tra sistemi interni ed esterni

Accessibilità ed inclusività

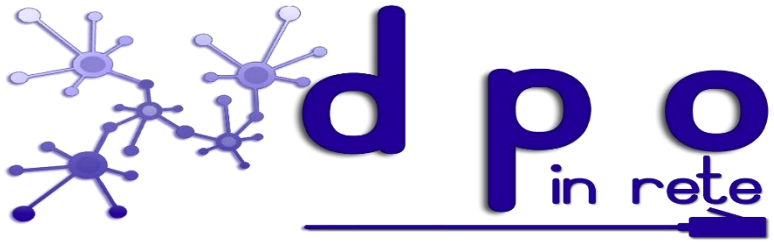
Formazione e sensibilizzazione

Ruolo del RPCT

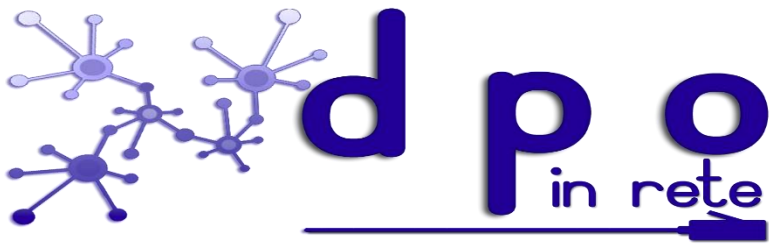
Valutazione e monitoraggi

Tempi di conservazione dei dati

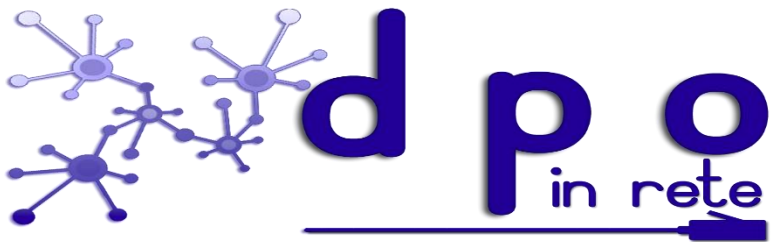
Vantaggi dell'attuazione di un sistema conforme



Ruolo del DPO nella gestione delle segnalazioni



Il Responsabile della Protezione dei Dati (DPO) svolge un ruolo importante nella gestione delle segnalazioni di irregolarità, assicurando che il trattamento dei dati personali all'interno del sistema di segnalazione sia conforme al GDPR e alle normative nazionali, come il D.lgs. n. 24/2023. La sua funzione si articola in diversi ambiti, che comprendono consulenza, monitoraggio e supporto operativo, garantendo che i diritti dei soggetti coinvolti siano tutelati e che le procedure siano in linea con i principi di legalità, trasparenza e riservatezza.



Consulenza sulla conformità normativa

Monitoraggio del trattamento dei dati

DPIA

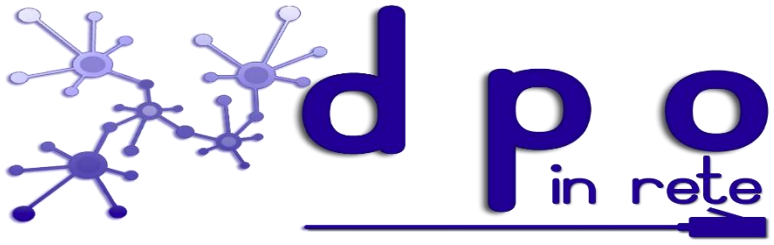
Garanzia della riservatezza

Collaborazione con altre funzioni

Gestione dei diritti degli interessati

Risoluzione delle criticità

Sensibilizzazione e formazione



Trattamento dei dati personali nelle segnalazioni



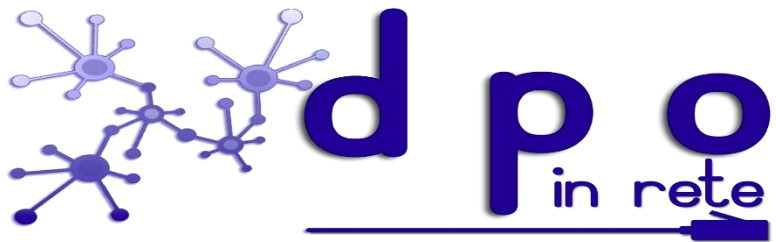
Il trattamento dei dati personali nelle segnalazioni è un componente centrale del sistema di segnalazione. Questo processo coinvolge diverse categorie di dati personali, incluse informazioni sul segnalante, sul segnalato e su eventuali terzi menzionati nella segnalazione.



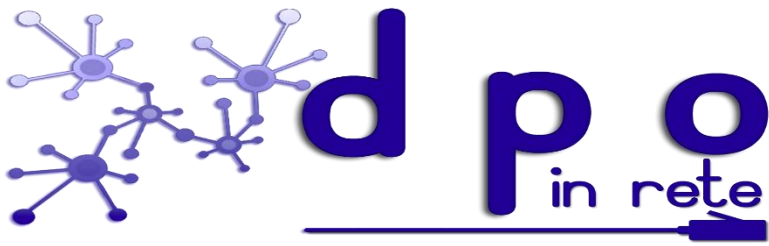
Dati personali del segnalante

Dati personali del segnalato

Dati personali di terzi



Tutela dell'anonimato e riservatezza



La tutela dell'anonimato e della riservatezza nel contesto delle segnalazioni è un aspetto fondamentale della disciplina del whistleblowing. Questa tutela è essenziale per garantire che i segnalanti possano denunciare illeciti o irregolarità senza timore di ritorsioni, favorendo così un sistema sicuro e affidabile. La normativa prevede misure rigorose per proteggere l'identità del segnalante e per garantire che tutte le informazioni raccolte siano gestite in modo conforme ai principi di riservatezza e protezione dei dati personali.



Anonimato del segnalante

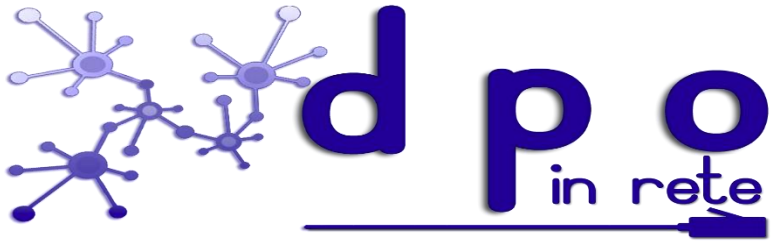
Riservatezza delle informazioni

Misure tecniche ed organizzative

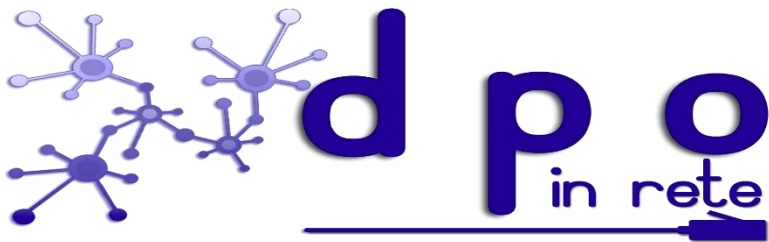
Situazioni di non garanzia dell'anonimato

Comunicazioni al segnalante sui propri diritti

Monitoraggio e supervisione



Misure di sicurezza per la protezione dei dati



Le misure di sicurezza per la protezione dei dati personali nel contesto delle segnalazioni di whistleblowing sono un elemento fondamentale per garantire la riservatezza e l'integrità delle informazioni trattate. Queste misure devono essere progettate per prevenire accessi non autorizzati, manipolazioni o perdite di dati.



Misure tecniche

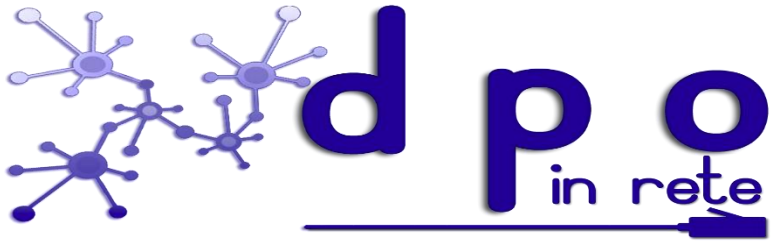
Misure organizzative

Protezione delle piattaforme digitali

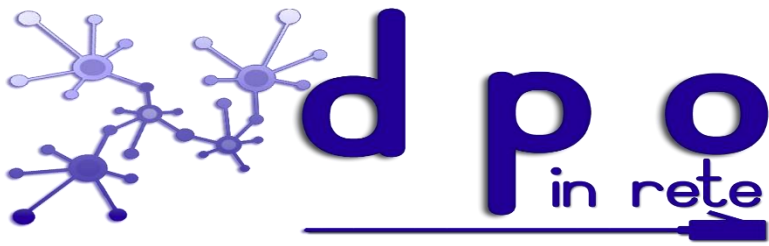
Monitoraggio e rilevazione

Gestione delle violazioni dei dati

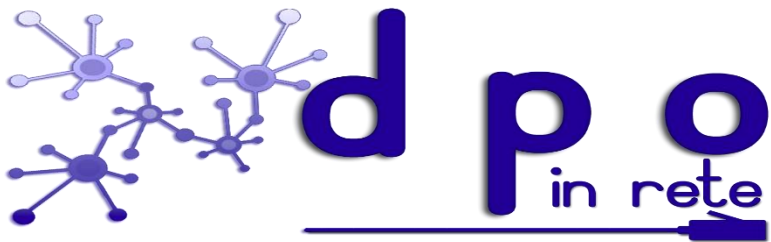
Controllo e audit



Diritti degli interessati e gestione delle richieste



La gestione dei diritti degli interessati nel contesto delle segnalazioni è particolarmente rilevante in quanto il rispetto di questi diritti, come quelli di accesso, rettifica, cancellazione e limitazione del trattamento, è essenziale per bilanciare la protezione dei dati personali con l'efficacia del sistema di segnalazione e le esigenze investigative.



Diritti degli interessati

Limitazioni al diritto di informazione

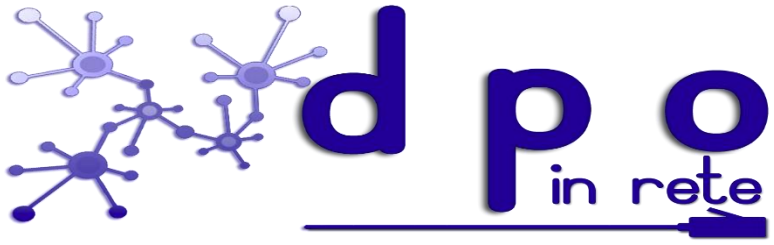
Gestione delle richieste

Bilanciamento tra diritti ed indagini

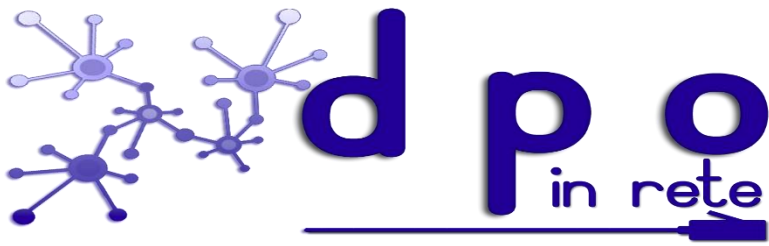
Protezione dei dati nelle risposte

Collaborazione con il DPO

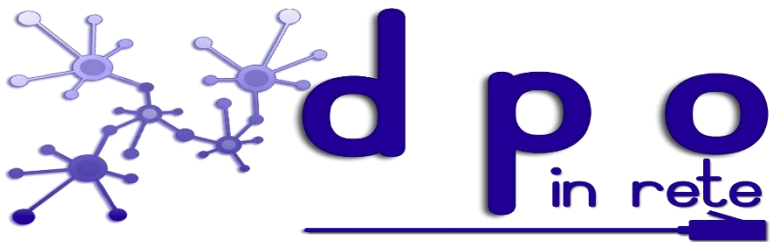
Reclami e ricorsi



Conseguenze legali e sanzioni



Le conseguenze legali e le sanzioni previste in caso di violazione delle norme sulla gestione delle segnalazioni di denuncia sono severe e progettate per garantire il rispetto delle disposizioni in materia di protezione dei dati personali e delle tutele dei segnalanti. Le sanzioni colpiscono sia le omissioni relative all'implementazione dei sistemi di segnalazione sia i comportamenti attivi che violano i principi normativi.



Mancata implementazione dei canali di segnalazione

Violazione della riservatezza

Ritorsioni contro il segnalante

Violazione delle norme sulla protezione dei dati

Obblighi di audit e vigilanza

Danni reputazionali

Ruolo delle Autorità di vigilanza

Rischio di procedimenti legali