PIATTAFORMA DI WHISTLEBLOWING

OpenBlow® è la piattaforma leader per le segnalazioni di condotte illecite destinata alle **Pubbliche Amministrazioni** e alle **Organizzazioni Private**, che ottempera in modo nativo alle direttive e alle norme di riferimento in materia di Whistleblowing e Privacy.

Nasce dalla collaborazione con l'Autorità Nazionale Anticorruzione (**ANAC**) e grazie a questa partnership, la piattaforma garantisce la piena conformità con tutti i **requisiti di legge in materia whistleblowing.**

La normativa

La **legge 179/2017** e il **D.lgs. 231/2001,** con cui in Italia si è iniziata a definire la disciplina in ambito whistleblowing, prevedevano già l'adozione di uno strumento informatico all'interno delle **Organizzazioni Pubbliche** e **Private**, attraverso il quale i dipendenti segnalano, a specifici individui o organismi (compresi organi di polizia e autorità pubbliche) una possibile frode, un reato, un illecito o qualunque condotta irregolare commessa da altri soggetti appartenenti all'organizzazione.

Il **30 marzo 2023 è entrato in vigore il decreto legislativo 24/2023 in attuazione della Direttiva (UE) 2019/1937**, 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". Il decreto ha ampliato il campo di applicazione e imposto l'obbligo di mettere a disposizione canali di segnalazione che garantiscano la protezione delle persone coinvolte e menzionate nella segnalazione e che ne consenta la gestione tempestiva ed efficiente.

I soggetti destinatari degli obblighi in materia di whistleblowing secondo la normativa sono individuati agli art. 2 e 3 del D.Lgs. 24/2023:

- **Soggetti del settore pubblico:** amministrazioni pubbliche, autorità amministrative indipendenti, gli enti pubblici economici, i concessionari di pubblico servizio, le imprese a controllo pubblico e le imprese in house, anche se quotate.

- **Soggetti del settore privato che:**

  1. hanno impiegato, nell'ultimo anno, **la media di almeno 50 lavoratori** subordinati con contratti di lavoro a tempo indeterminato o determinato;

  2. rientrano nell'ambito di applicazione degli atti dell'Unione di cui alle parti I.B e II dell'allegato al decreto, **anche se nell'ultimo anno non hanno raggiunto la media di 50 lavoratori subordinati;** si tratta dei settori dei servizi, prodotti e mercati finanziari, prevenzione del riciclaggio e del finanziamento del terrorismo, nonché della sicurezza dei trasporti;

  3. sono diversi dai soggetti di cui al punto precedente, sono dotati di un modello di organizzazione **e gestione 231,** anche se nell'ultimo anno non hanno raggiunto la media di 50 lavoratori subordinati.

INFO@LASERROMAE.IT

I PUNTI DI FORZA

La **piattaforma di OpenBlow è un'applicazione Web-Based** ed è accessibile da qualsiasi PC e dispositivo mobile.

- Piattaforma informatica **Web-Based.**
- **Semplificazione** delle procedure di gestione delle segnalazioni.
- **Contenuto** delle segnalazioni **riservato** e **cifrato.**
- **Separazione dell'identità** del segnalante dalla segnalazione.
- Adeguate politiche di **accesso** e **conservazione dei dati.**
- **Integrazione** della piattaforma in ambienti preesistenti.
- **Disponibile** in qualsiasi lingua.

Tutela del Whistleblower

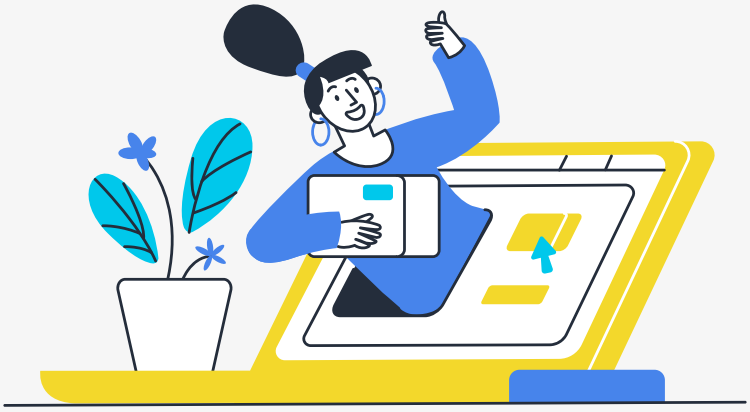
Il D.Lgs. 24/2023 riconosce ai Whistleblower un sistema di protezione per la **tutela della riservatezza della propria identità,** per la tutela da eventuali ritorsioni e la **non punibilità dei segnalanti** legate al segreto industriale (art. 54 bis del d.lgs. n. 165/2001).

- **Tutela della riservatezza dell'identità del segnalante.**
  L'identità del segnalante non può essere rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni.

  La protezione riguarda non solo il nominativo del segnalante ma anche tutti gli elementi della segnalazione dai quali si possa ricavare, anche indirettamente, l'identificazione del segnalante;

- **Tutela da eventuali misure ritorsive o discriminatorie a seguito di una segnalazione**
  Qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile, o della divulgazione pubblica e **che provoca o può provocare, alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto, da intendersi come danno ingiustificato.**

- **Non punibilità dei segnalanti**
  Non è punibile chi rivela o diffonde informazioni sulle violazioni coperte dall'obbligo di segreto, diverso da quello professionale forense e medico, o relative alla tutela del diritto d'autore o alla protezione dei dati personali ovvero se, al momento della segnalazione, denuncia o divulgazione, aveva ragionevoli motivi di ritenere che la rivelazione o diffusione delle informazioni fosse necessaria per effettuare la segnalazione e la stessa è stata effettuata nelle modalità richieste dalla legge.



OBIETTIVO

L'obiettivo del Whistleblowing è quello di permettere alle Organizzazioni di affrontare i problemi segnalati in modo tempestivo ed efficace, redendo note situazioni di rischio o di danno e contribuendo alla prevenzione e al contrasto di eventuali illeciti.

- **Attori del Whistleblowing**
  I principali attori coinvolti nel processo di Whistleblowing interagiscono fra di loro in modalità sicura e riservata attraverso la piattaforma OpenBlow®.
- **Trattazione delle segnalazioni**
  La gestione delle segnalazioni di condotte illecite è organizzata per fasi di trattazione sequenziali, strutturate all'interno di un processo implementato e completamente automatizzato attraverso la piattaforma.

Processo di Whistleblowing

Il processo di Whistleblowing è centralizzato sulla piattaforma, la quale garantisce una chiara separazione dei ruoli e la sicurezza durante tutte le fasi di gestione della segnalazione.
Alla ricezione di una segnalazione, la persona designata procede con i seguenti passi:

- **Categorizzazione** della segnalazione;
- **Verifica preliminare** della segnalazione (screening della segnalazione);
- **Istruttoria** (e iterazione con il Segnalante);
- **Definizione** (chiusura) con esito di archiviazione o di inoltro;
- **Trasmissione agli Uffici Competenti** e/o dipartimenti interni in caso di inoltro.

01.
INSERIMENTO SEGNALAZIONE

02.
VERIFICA PRELIMINARE

03.
ISTRUTTORIA

04.
FLUSSI CON ALTRI ATTORI

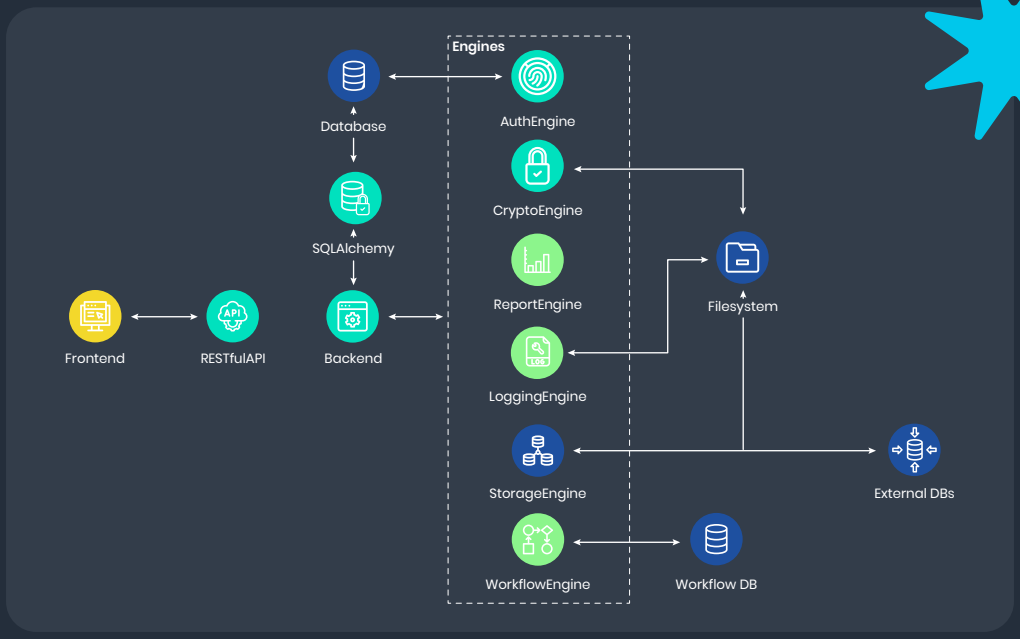
INFO@LASERROMAE.IT

La piattaforma

La piattaforma di Whistleblowing è stata progettata e implementata dal team di sviluppo della Laser Romae, con l'obiettivo di realizzare un prodotto sicuro, semplice da utilizzare ed integrabile in qualsiasi tipo di Organizzazione.

Architettura della piattaforma

La piattaforma ha un'architettura multi-engine, per permettere la facile integrazione in ambienti eterogenei. La modularità della piattaforma consente, per ognuna delle funzionalità core, di poter utilizzare dei plugin per collegarsi a sistemi pre-esistenti (ad esempio BPMN, sistemi di code, sistemi di storage).



Modalità di erogazione

Il servizio di Whistleblowing è erogato sia in modalità **SaaS** (Software as as Service) sia in modalità **on-premise** sulle infrastrutture del Cliente.

▶ **Saas**
Il servizio di Whistleblowing è erogato in modalità SaaS attraverso i Datacenter della Laser Romae localizzati in Europa.

Caratteristiche del servizio:
- Provisioning dell'infrastruttura
- Deployment della piattaforma
- Esercizio della piattaforma
- Formazione del personale
- Supporto
- Manutenzione correttiva e adeguativa
- Manutenzione evolutiva
- Dismissione del servizio
- Migrazione dati

▶ **On-premise**
La piattaforma di Whistleblowing può essere installata on-premise sui Datacenter del Cliente e integrata all'interno dell'infrastruttura.

Caratteristiche del servizio:
- Installazione della piattaforma
- Configurazione / Tuning della piattaforma
- Esercizio della piattaforma
- Formazione del personale
- Supporto
- Manutenzione correttiva e adeguativa
- Manutenzione evolutiva
- Migrazione dati

LA PIATTAFORMA

La piattaforma oltre a consentire la segnalazione degli illeciti utilizzando modalità digitali, ottempera in modo nativo alle **direttive ANAC** e alle norme di riferimento:

- **separare l'identità del segnalante dal contenuto della segnalazione**, prevedendo l'adozione di codici sostitutivi dei dati identificativi, in modo che la segnalazione possa essere processata in modalità anonima e rendere possibile la successiva ricostruzione dell'identità del segnalante nei soli casi consentiti;
- **gestire le segnalazioni in modo trasparente** attraverso un iter procedurale definito e comunicato all'esterno con termini certi per l'avvio e la conclusione dell'istruttoria;
- mantenere **riservato il contenuto delle segnalazioni** durante l'intera fase di gestione della segnalazione;
- adottare **protocolli sicuri per il trasporto dei dati in rete** nonché l'utilizzo di strumenti di crittografia per i contenuti delle segnalazioni e dell'eventuale documentazione allegata;
- adottare **adeguate modalità di conservazione dei dati** e della documentazione (fisico, logico, ibrido);
- adottare **politiche di tutela della riservatezza** attraverso strumenti informatici (disaccoppiamento dell'identità del segnalante rispetto alle informazioni relative alla segnalazione, crittografia dei dati e dei documenti allegati);
- adottare **politiche di accesso ai dati** (funzionari abilitati all'accesso, amministratori del sistema informatico).

Sicurezza

Relativamente agli aspetti legati alla Cyber Security, ANAC ha richiesto l'esecuzione di un Application Security Assessment (ISO 27001, OWASP) della piattaforma negli ambienti di pre-esercizio ed esercizio.

Le principali caratteristiche di sicurezza della piattaforma sono:

- **Data retention policy**
  Ogni segnalazione memorizzata nel Database incrementa l'attrattiva per potenziali Hacker.
  Le segnalazioni hanno una data di scadenza che può essere estesa dal Receiver.
  Una segnalazione scaduta viene rimossa insieme a tutti i suoi dati.
- **Server resiliency**
  Il Server è configurato in modo da rendere inoffensivi attacchi di tipo D/DOS.
  Richieste massive provenienti da uno stesso indirizzo IP che possano configurarsi come attacco, sono automaticamente inibite.
- **Password storage**
  Le password sono memorizzate attraverso l'utilizzo di un Hash generato con un salt a 128 bit casuale.
  Le ricevute dei segnalanti sono crittografate utilizzando il modulo Crypto.
  Random di Python con il quale viene generato un codice di 16 cifre.
- **Web content security**
  La comunicazione tra front end e back end utilizza le best practice, condivise a livello internazionale, tra cui header di sicurezza e cifratura della comunicazione con TLS 1.3.
- **File encryption**
  Gli allegati della segnalazione, insieme alla segnalazione stessa, vengono cifrati utilizzando il Crypto Engine selezionato. Di default viene offerta una cifratura AES 256.
- **GDPR**
  La Piattaforma di Whistleblowing è a norma con il regolamento generale sulla protezione dei dati (GDPR – General Data Protection Regulation, regolamento UE 2016/679).