Informazioni generali sulla piattaforma informatica per le segnalazioni di Whistleblowing

(DECRETO LEGISLATIVO 10 marzo 2023, n. 24)

1 Premessa

La piattaforma per la gestione del Whistleblowing, ***www.bonzispa.segnalazioni.net***, è lo strumento informatico messo a disposizione dei Segnalanti e del Gestore delle segnalazioni di Whistleblowing, finalizzato a gestire le segnalazioni di illeciti o di violazioni relative al Modello di Organizzazione e Gestione 231.

La piattaforma è conforme alla normativa vigente in materia:

- Linee guida in materia di Whistleblowing: Delibera ANAC n. 469 del 9 giugno 2021;
- Decreto Legislativo del 10 Marzo 2023 n. 24 "Attuazione della Direttiva (UE) 1937/2019 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";
- Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (Regolamento generale del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali).

2 Riferimenti normativi

Il D.lgs. 10 Marzo 2023, n. 24, recante le norme di attuazione della Direttiva (UE) 2019/1937 del 23 ottobre 2019, disciplina la protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato.

Il Decreto impone a tutte le aziende private con una media nell'ultimo anno di almeno 50 dipendenti a tempo determinato o indeterminato, l'istituzione di canali interni sicuri per la segnalazione degli illeciti.

3 La segnalazione

Il Segnalante (o Whistleblower) può:

- accedere in maniera riservata e sicura al sistema in **Modalità Riservata,** registrandosi al sistema per l'invio di una segnalazione scritta "nominativa e con gestione dell'identità riservata" (c.d. utente registrato);
- inserire la propria segnalazione scritta tramite una procedura intuitiva e di facile compilazione;
- inviare la segnalazione tramite la piattaforma web;
- seguire la segnalazione e visualizzare lo stato di lavorazione della segnalazione;
- scambiare messaggi con il soggetto Gestore della segnalazione;
- ricevere via e-mail avvisi di risposta alla propria segnalazione e ai messaggi.

4 Il form di segnalazione

I campi da compilare per la segnalazione scritta sono i seguenti:

- informazioni illecito;
- oggetto;
- tipologia segnalante (rapporto del segnalante con l'Organizzazione);
- natura Illecito (elenco di valori preimpostati configurabili e selezionabili tramite menu a tendina);
- soggetti coinvolti;
- autori illecito;
- persone informate;
- luoghi e date;
- unità organizzativa/e delle persone coinvolte;
- luogo in cui si è verificato il fatto;

- data (anche presunta) in cui si è verificato il fatto;
- data (anche presunta) di conclusione del fatto;
- descrizione dei fatti;
- allegati (con controllo dell'estensione degli allegati, al fine di limitare l'upload solo alle estensioni consentite).

5 Ambiente di amministrazione

L'ambiente di amministrazione consente al Gestore della segnalazione di:

- ricevere via e-mail un avviso di presenza di segnalazione nel sistema;
- gestire lo stato di lavorazione della segnalazione;
- scambiare messaggi con il segnalante per eventuale richiesta di documentazione e integrazioni;

6 Sicurezza e riservatezza

Sulla piattaforma tutte le informazioni che possono rivelare i contenuti di una segnalazione e l'identità del suo autore o che possono dare indicazioni sull'attività di un segnalante, sono protette da un sistema di cifratura.
Le segnalazioni (comprese le bozze), gli allegati (anche quelli temporanei), i log di attività e le sessioni sono cifrati.
Il processo di registrazione del Segnalante è separato dalla segnalazione, il che consente la gestione delle segnalazioni riservate in maniera anonima: non esiste alcuna correlazione diretta tra Segnalante e contenuto della segnalazione.
Il sistema è installato su una infrastruttura di Server Dedicati certificata TIER IV1, che garantisce le migliori prestazioni in termini di sicurezza e di disponibilità dei dati.

6.1 Caratteristiche tecniche del sistema di cifratura

6.1.1 Gestione password per autenticazione

Le password non sono memorizzate in chiaro nel database, in maniera da impedirne un eventuale, seppure improbabile, furto o visualizzazione. Nemmeno gli amministratori di sistema possono risalire alla password in quanto queste sono memorizzate in modalità cifrata, in combinazione con un salt random, nel database di sistema con algoritmo Hash SHA512.
Non è possibile, partendo dall'hash, ricalcolare la password originale.

6.1.2 Autenticazione a due fattori (strong authentication)

L'accesso al sistema deve essere confermato tramite inserimento di un codice inviato dal sistema all'indirizzo email dell'utente. L'opzione può essere disabilitata dall'utente stesso.

6.1.3 Cifratura dei contenuti

Tutte le informazioni che possono rivelare i contenuti di una segnalazione e l'identità del suo autore o che, al limite, possono dare indicazioni sull'attività di un segnalante, sono protette e cifrate a più livelli.

6.1.4 Gestione della password in fase di sessione

Le password non vengono trascritte in chiaro, ma il software provvede a criptare la parte di sessione relativa alla password durante l'utilizzo della piattaforma da parte degli utenti.
Per aumentare ulteriormente il livello di protezione di questo dato, la sessione viene quindi cifrata con l'algoritmo AES-256-CBC utilizzando una chiave di cifratura generata dal client dell'utente. Ulteriore misura di sicurezza è l'assenza sul server di un'associazione tra la sessione e l'utente. Una volta scaduta la sessione, questa viene eliminata dal sistema.

Castenedolo, lì 17 dicembre 2023

Il Titolare del trattamento
Bonzi S.p.A.
Andrea Beschi
(Amministratore Unico)