IL WHISTLEBLOWING

ovvero i sistemi che consentono ad una persona di segnalare in maniera anonima e sicura, illeciti e/o comportamenti non etici:

- corruzione
- reati
- parità di genere
- mobbing

PI COMPUTERS

QUALI SONO I CANALI DI SEGNALAZIONE

canali di segnalazione interna, implementati dagli enti del settore privato o dalle amministrazioni pubbliche

INTERNI

canale di segnalazione esterna, attivato dall'Autorità Nazionale Anticorruzione (ANAC) se il canale interno è non presente/obbligato o non funzionante/rapido (PERICOLO!!)

ESTERNI

divulgazioni pubbliche, tramite i mass media in caso di pericolo imminente o inadempienze/pericoli ai punti precendenti (CASO WATERGATE)

DIVULGAZIONI PUBBLICHE

PI COMPUTERS

E IL GDPR?

Ogni trattamento dei dati personali connesso alla gestione dei canali di segnalazione deve essere eseguito a norma del GDPR

BASE GIURIDICA

Il Titolare del trattamento deve adottare idonee misure di protezione volte a garantire la riservatezza circa l'identità del segnalante

MISURE DI SICUREZZA

Principio di minimizzazione
Esercizio dei Diritti
Privacy by design e privacy by default
Data Retention

REGISTRO DEI TRATTAMENTI

CHI SI DEVE DOTARE DEL SISTEMA DI SEGNALAZIONE?

- A Prescindere dalla Dimensione TUTTI GLI ENTI PRIVATI che operano nei settori :
  - FINANZIARIO (ad esempio FINTECH)
  - TRASPORTI
  - Che adottano un MODELLO 231
- TUTTI GLI ENTI PRIVATI da 50 a 249 dipendenti
- TUTTI GLI ENTI PRIVATI che hanno 250 dipendenti o più
- TUTTI GLI ENTI PUBBLICI

PI COMPUTERS

Obbligo di stabilire canali di segnalazione interni e per relativo seguito

ART 8

- Invio della segnalazione scritta
- Segnalazione telefonica
- Coordinamento delle misure di follow-up
- Identificazione della voce del segnalante nei messaggi vocali resa irriconoscibile tramite un programma di "morphing"
- Notifica al segnalante prima della registrazione della segnalazione

Segnalazione orale, scritta

ART 9

- Invio della Segnalazione telefonica
- Creazione di un clima di fiducia grazie al trattamento trasparente e sicuro dei dati del segnalante

Garantire la riservatezza dell'identità della persona segnalante e degli eventuali terzi citati

Obbligo di riservatezza

ART 9

- Massima sicurezza di accesso garantita (massimi standard di sicurezza informatica, robusti algoritmi di crittografia, server certificato EuroPriSe)
- Certificazione ISO 27001
- Elevata granularità nella creazione e
- Gestione di diritti di accesso e ruoli
- Possibilità di anonimizzazione conformemente alla normativa riguardante la protezione dei dati
- Raccomandazioni per i segnalanti per tutelare l'anonimato
- Dialogo sicuro grazie alla casella di posta protetta
- I moduli di testo facilitano la conferma di ricezione e la comunicazione di feedback ai segnalanti
- Reminder impostabili per rispettare le scadenze

PI COMPUTERS

Trattamento dei dati personali in conformità con il Regolamento GDPR Generale sulla Protezione dei Dati (GDPR) e la precedente Direttiva

Nessuna raccolta di dati non utili o cancellazione senza indugio dei dati

ART. 17

- Impostazioni predefinite di comprovata conformità alla protezione dei dati
- Il motivo principale della segnalazione e domande predefinite impediscono la raccolta di dati non rilevanti
- Sistema di segnalazione a norma di GDPR

Revisione, correzione e conferma della trascrizione di una segnalazione telefonica

Conservazione di tutte le segnalazioni in arrivo nel rispetto degli obblighi di riservatezza

Conservazione fino all'adempimento dei requisiti della Direttiva / del diritto dell'Unione / diritto nazionale

ART .18

- Documentazione salvata e archiviata in maniera conforme e a prova di audit
- Efficacia misurabile grazie a un sistema di reporting customizzabile
- Dopo l'anonimizzazione, segnalazione archiviabile per un periodo di tempo illimitato
- Revisione, correzione e conferma della segnalazione telefonica grazie a sistemi di comunicazione con i segnalanti

PI COMPUTERS

Ancora più attenzione deve essere posta sulla sicurezza dei dati che vengono raccolti.

Non si possono usare mezzi di comunicazione informatici potenzialmente non sicuri (es. email) da e verso il segnalante.

E' consigliabile prevedere meccanismi di cancellazione dei log di sistema relativi agli accessi alla piattaforma informatica (vedi sanzione Garante del 11/05/2022).

Cifratura del canale di

- I dati viaggiano in maniera sicura utilizzando protocolli e standard appositi (es. HTTPS).

Cifratura dei dati su DB o

- L'applicativo prevede la criptazione dei dati della

Caratteristiche tecniche

Supporto multi-sito che consente di eseguire più siti virtuali sulla stessa configurazione
Interfacce utente reattive realizzate con Boostrap CSS Framework
Supporto di accessibilità integrato con conformità WAI-ARIA
Misurazione automatizzata della qualità del software e test di integrazione continua
Piano di supporto a lungo termine (LTS)
Costruito con tecnologie framework leggere (AngularJS e Python Twisted)
Database SQLite integrato
Configurazione automatica di Tor Onion Services versione 3
Supporto per l'iscrizione self-service per la configurazione del servizio SaaS di segnalazione di irregolarità
Supporto per il sistema operativo Linux (Debian/Ubuntu)
Pacchetto Debian con repository per aggiornamenti/aggiornamenti
Applicazione completamente autonoma
Facile integrazione della piattaforma con i siti web esistenti

PI COMPUTERS