Atto organizzativo di attuazione della disciplina del Whistleblowing

Il presente atto organizzativo stabilisce e regola le modalità operative con cui il Comune di Montorso Vicentino applica l'istituto del Whistleblowing di cui all'art. 54 bis D.Lgs. 165/2001 in piena conformità alle linee guida approvate dall'ANAC con Delibera n. 469 del 9 giugno 2021.

1. L'informazione e la formazione

Il Comune di Montorso Vicentino promuove la cultura della legalità, anche informando e formando il proprio personale sul tema e sulla normativa riferita al Whistleblowing, con opportune iniziative da svolgersi almeno annualmente. Tali momenti informativi/formativi possono essere estesi anche a particolari categorie di soggetti esterni e a tutta la comunità amministrata.

2. La modalità di acquisizione e gestione delle segnalazioni

Il Comune di Montorso Vicentino si è dotato di un sistema tecnologico per la ricezione e gestione delle segnalazioni di condotte illecite denominato "Whistleblowing Intelligente". Nella home page del sito istituzionale dovrà essere riportata l'informazione riguardante le modalità operative utilizzabili per raggiungere via web la piattaforma di segnalazione di condotte illecite
Le Segnalazioni possono essere anche inviate alla piattaforma messa a disposizione da ANAC digitando il seguente URL:
https://servizi.anticorruzione.it/segnalazioni/#!/#%2F
Le segnalazioni devono essere inviate unicamente alla piattaforma di ANAC qualora il segnalante ravvisi un conflitto di interesse tra il contenuto della segnalazione e il RPCT o altra persona da lui indicata per l'esame della segnalazione.
Le segnalazioni di misure ritorsive nei confronti di chi ha fatto una segnalazione di whistleblowing, devono essere inviate esclusivamente tramite la piattaforma messa a disposizione dall'ANAC

3. La presentazione della segnalazione

Possono effettuare segnalazioni di condotte illecite cliccando sull'apposito pulsante nella pagina web https://wb.anticorruzioneintelligente.it/anticorruzione/index.php?codice=ZAIYLM&dipendente=1 qualificandosi obbligatoriamente attraverso il sistema SPID:

- tutti coloro che hanno in essere un rapporto di lavoro dipendente con il Comune di Montorso Vicentino

- i dipendenti e collaboratori delle imprese fornitrici nel caso in cui la segnalazione riguardi fatti in cui è coinvolto o che riguardino Montorso Vicentino.

Eventuali segnalazioni pervenute da altri soggetti non saranno prese in considerazione. In tali casi le segnalazioni verranno archiviate in quanto mancanti del requisito soggettivo (oppure saranno prese in considerazione solo se ben dettagliate e circostanziate e comunque secondo l'insindacabile giudizio del RPCT).

Il Comune di Montorso Vicentino ha attivato un secondo canale di ricezione delle segnalazioni di condotte illecite (link: https://wb.anticorruzioneintelligente.it/anticorruzione/index.php?codice=ZAIYLM&dipendente=0) in cui non è richiesta l'identificazione tramite SPID e non è obbligatorio inserire i dati relativi all'identità del segnalante. In questo caso non potranno essere concesse al segnalante le tutele previste dalla legge e la segnalazione verrà presa in considerazione solamente nei casi in cui essa appare ben circostanziata e rilevante.

Il segnalante è tenuto a compilare in modo esaustivo chiaro, preciso e circostanziato le sezioni del modulo di segnalazione, fornendo le informazioni richieste come obbligatorie e il maggior numero possibile di quelle facoltative.

Al segnalante si richiede un comportamento collaborativo tenendo costantemente aggiornato Montorso Vicentino in ordine all'evoluzione della propria segnalazione/comunicazione secondo le modalità più avanti illustrate.

All'invio della segnalazione, la piattaforma presenta al segnalante una videata con il codice univoco di segnalazione, necessario per:

- integrare/aggiornare in un secondo momento quanto riportato nel modulo di segnalazione
- rispondere ad eventuali richieste di chiarimenti/approfondimenti
- verificare l'avanzamento dell'iter di gestione della segnalazione.

Il codice univoco di segnalazione non può essere rigenerato dalla piattaforma. Pertanto il segnalante dovrà conservarlo con cura per poter rientrare nella segnalazione al fine di verificarne l'iter di esame, per rispondere ad eventuali richieste del RPCT o, ancora, per integrare spontaneamente le informazioni già sottoposte all'attenzione del RPCT

4. La ricezione della segnalazione

Alla ricezione della segnalazione, la piattaforma compie automaticamente le seguenti azioni:

- attribuisce alla segnalazione un numero progressivo e la data di ricezione

- invia alla casella di posta elettronica indicata dal RPCT in fase di impostazione, un messaggio di avviso. Nessuna informazione circa il contenuto della segnalazione sarà inviata via mail
- invia al segnalante l'avviso che la segnalazione è stata correttamente acquisita dal sistema, se è stato indicato nel modulo di segnalazione un indirizzo di posta elettronica.
-

5. L'analisi preliminare

L'analisi preliminare dovrà essere compiuta entro 15 gg. lavorativi dalla data di ricezione della segnalazione e ha lo scopo di accertare le condizioni al fine di assegnare le tutele al segnalante da un lato e, dall'altro, se sussistono i requisiti essenziali per eseguire la fase istruttoria.

Per compiere l'analisi preliminare della segnalazione, il RPCT si autentica sulla piattaforma al seguente URL https://wb.anticorruzioneintelligente.it/login.php digitando nome e password o, in alternativa, attraverso il sistema SPID.

Nell'apposita sezione della piattaforma, il RPCT individua ed entra nella nuova segnalazione prendendone visione. I dati riferiti all'identità del segnalante non sono visibili.

La piattaforma mette la segnalazione in stato "Analisi preliminare" ed invia al segnalante (se questi ha lasciato i suoi riferimenti di posta elettronica) una notifica di passaggio di stato della segnalazione).

Il RPCT può procedere all'esame preliminare o assegnare l'esame della segnalazione ad un suo collaboratore precedentemente indicato e registrato nella piattaforma alla quale potrà accedere attraverso nome e password o attraverso il sistema SPID.

Colui che esamina la segnalazione può comunicare con il segnalante attraverso la piattaforma, chiedendo integrazioni, chiarimenti, ulteriori informazioni eccetera. Il messaggio inviato al segnalante interrompe automaticamente il conteggio del tempo necessario per concludere la fase di analisi preliminare. Il conteggio del tempo riprenderà automaticamente al momento in cui il segnalante risponde con un messaggio all'interno della piattaforma alle richieste ricevute. Alla risposta del segnalante, il RPCT ed eventualmente il collaboratore designato, vengono immediatamente avvertiti con un messaggio in posta elettronica senza riportare nessun dato o informazione utile a rivelare il contenuto della segnalazione o sue parti. Decorsi 30 gg. senza ricevere alcuna risposta, il RPCT riprende l'iter di valutazione con le informazioni disponibili

La segnalazione verrà posta in stato "Istruttoria" se il RPCT/designato non ravvisa nessuno dei seguenti elementi, in caso contrario la segnalazione sarà archiviata con relativa motivazione:

- Manifesta mancanza di interesse all'integrità della pubblica amministrazione
- Manifesta incompetenza dell'ente sulle questioni segnalate
- Manifesta infondatezza per l'assenza di elementi di fatto idonei a giustificare accertamenti

- Accertato contenuto generico della segnalazione tale da non consentire la comprensione dei fatti
- Segnalazione corredata da documentazione non appropriata o inconferente
- Produzione di sola documentazione senza descrizione esaustiva dei fatti e/o elementi essenziali.

Il segnalante sarà avvertito con messaggio in posta elettronica del cambiamento di stato della segnalazione e, se chiusa, delle motivazioni.

6. La fase istruttoria

La fase istruttoria può durare fino ad un massimo di 60 giorni di calendario. Durante questa fase, il RPCT e/o il collaboratore indicato in precedenza, avranno la possibilità di tenere all'interno della piattaforma un diario in riferimento alle attività istruttorie effettuate ed, inoltre, sarà possibile scrivere la relazione delle risultanze delle attività istruttorie senza ricorrere al download/upload di file.

Anche in questa fase è possibile, come descritto nella fase precedente, attivare un dialogo a distanza tra RPCT/designato e segnalante. L'invio di un messaggio da parte del RPCT/designato, interrompe il conteggio dei giorni utili per la conclusione della fase istruttoria. Decorsi 30 gg. giorni senza aver ricevuto risposta, il RPCT/designato può decidere di proseguire l'istruttoria avvalendosi dei soli elementi disponibili. Al termine dell'istruttoria la segnalazione sarà messa in stato "Chiusa" indicando la motivazione e l'azione seguente compiuta, ovvero archiviata oppure inviata ad uno o più delle seguenti sedi competenti:

- ufficio provvedimenti disciplinari
- ANAC
- Corte dei conti
- Autorità giudiziaria

Nel caso in cui il RPCT invii la segnalazione all'Ufficio provvedimenti disciplinari o ad altra autorità, egli ricava i dati e ogni altro elemento che possa, anche indirettamente, consentire l'identificazione del segnalante, evidenziando che, trattandosi di una segnalazione ex art 54-bis, è necessario garantire la riservatezza dell'identità del segnalante.

Poiché nella documentazione trasmessa potrebbero essere presenti dati personali di altri interessati, i soggetti che trattano i dati sono comunque "autorizzati" al riguardo (artt. 4, par.1, n. 10, 29, 32 e par. 4 del Regolamento UE 2016/679).

7. Le modalità di accesso alla segnalazione da parte del segnalante

Il segnalante può integrare/aggiornare le informazioni già riportate nel modulo di segnalazione, oppure può prendere visione dell'iter di esame della segnalazione ed eventuali messaggi ricevuti da parte del RPCT/designato, entrando nella piattaforma secondo le modalità già indicate e inserendo il codice univoco di segnalazione dopo aver fatto clic sul pulsante "Verifica stato segnalazione".
Se il segnalante ha inserito un indirizzo di posta elettronica all'interno del modulo di segnalazione, la piattaforma provvederà ad inviare via email tutte le notifiche di cambio stato della segnalazione ed eventuali richieste di informazioni/integrazioni da parte del RPCT/designato. All'interno della mail sarò presente anche un link che consentirà di accedere automaticamente alla segnalazione senza dover digitare il codice univoco.

8. Il Custode dell'identità del segnalante e l'accesso ai dati

Il RPCT svolge anche il ruolo di Custode dell'identità del segnalante e ha sempre la possibilità di accedere ai dati identificativi del segnalante per gli usi consentiti o richiesti dalla legge.
L'accesso ai dati identificativi del segnalante da parte del RPCT è motivato e la motivazione viene registrata all'interno della piattaforma.
Il Segnalante riceve avviso delle motivazioni per le quali i suoi dati identificativi sono stati messi in chiaro.
Il RPCT/designato ha comunque la possibilità di ri-oscurare i dati relativi al segnalante in modo tale da poter esportare in PDF la segnalazione, qualora ne ravvisi la necessità, senza rendere visibili i dati identificativi del segnalante
La segnalazione e la documentazione ad essa allegata sono sottratte al diritto di accesso agli atti amministrativi previsto dagli artt. 22 e seguenti della legge 241/1990; escluse dall'accesso civico generalizzato di cui all'art. 5, co. 2, del d.lgs. 33/2013 nonché sottratte all'accesso di cui all'art. 2-undecies co. 1 lett. f) del codice in materia di protezione dei dati personali
Laddove l'Autorità giudiziaria per esigenze istruttorie volesse conoscere il nominativo del segnalante, il responsabile della prevenzione della corruzione e della trasparenza provvede a comunicare l'identità del segnalante, così come previsto dalle disposizioni di legge. È opportuno precisare che il whistleblower è preventivamente avvisato, attraverso l'informativa presente nel modulo di segnalazione, della eventualità che la sua segnalazione potrà essere inviata all'Autorità giudiziaria ordinaria e contabile.

9. Il consenso a rivelare l'identità del segnalante nell'ambito del procedimento disciplinare

Qualora si rendesse necessario, il segnalante ha la possibilità di esprimere chiaramente e

inequivocabilmente il consenso a rivelare le sue generalità nell'ambito di un procedimento disciplinare originatosi a seguito della segnalazione. Il Segnalante, quando rientra nella segnalazione, ha a disposizione un pulsante con il quale può acconsentire o meno a rivelare la sua identità nell'ambito del procedimento disciplinare. In caso in cui egli esprima il suo consenso, tale scelta non sarà più revocabile.

La piattaforma registra e rende visibile data e ora in cui è stato accordato il consenso. Appena espresso il consenso, la piattaforma invia un messaggio al RPCT per informarlo della scelta avvenuta da parte del segnalante.

10. La perdita delle tutele

Il comma 9 dell'art. 54-bis stabilisce che la tutela non è più garantita nel caso in cui il whistleblower non svolga la segnalazione in buona fede, precisando che la protezione per quest'ultimo viene meno ove sia accertata, anche con sentenza di primo grado, la sua responsabilità penale per i reati di calunnia o diffamazione o per quelli comunque commessi con la segnalazione, ovvero la sua responsabilità civile, nei casi di dolo o colpa grave.

Laddove la sentenza di condanna in primo grado dovesse essere riformata in senso favorevole al segnalante nei successivi gradi di giudizio, quest'ultimo potrà ottenere nuovamente la tutela prevista dall'art. 54-bis solo a seguito del passaggio in giudicato della pronuncia che accerta l'assenza della sua responsabilità penale per i reati di calunnia e/o diffamazione e/o commessi con la segnalazione.

Solo dove intervenga, in sede giudiziaria, l'accertamento della responsabilità per dolo o colpa grave in merito alla condotta calunniosa o diffamatoria messa in atto attraverso la segnalazione, il Comune di Montorso Vicentino potrà sanzionare disciplinarmente il segnalante

11. La durata di conservazione e possibilità di accesso alla segnalazione

La segnalazione sarà resa disponibile tanto al segnalante tanto al RPCT per 5 anni. Indipendentemente dallo stato della segnalazione, Segnalante e RPCT potranno utilizzare la chat asincrona contenuta nel modulo di segnalazione anche quando a segnalazione già esaminata.

12. Gli obblighi di sicurezza

Il RPCT e gli eventuali designati al trattamento delle segnalazioni sono obbligati alla riservatezza e a non rivelare a nessun altro, se non nei casi previsti dalla legge, l'identità del segnalante. Restano

ferme le responsabilità disciplinari previste per violazione degli appositi doveri di comportamento e per violazione delle norme sulla tutela dei dati personali.
La Società Tecnolink S.r.l. è ideatrice e proprietaria della piattaforma Whistleblowing Intelligente e si occupa di fornire il software in modalità Software as a Service (SaaS). La Tecnolink S.r.l nella persona del suo legale rappresentante pro tempore, è stata nominata Responsabile esterno del trattamento dei dati personali. Il Comune di Montorso Vicentino, nell'ambito di quanto previsto nell'atto di nomina, verifica e controlla le modalità operative con cui il Responsabile esterno assicura il trattamento dei dati personali in piena conformità a quanto previsto **dal REGOLAMENTO (UE) 2016/679 in particolar modo per le parti richiamate dalle Linee Guida ANAC in materia di Whistleblowing adottate con delibera** n. 469 del 9 giugno 2021. (per un dettaglio delle misure di sicurezza adottate dal Responsabile esterno del trattamento dati, vedi l'Allegato 2)

Allegato 2

Responsabile esterno del trattamento dei dati personali

Dati di contatto del Responsabile esterno del trattamento dei dati:

- Sede Legale: Via P. Bagetti, 10 – 10143 Torino
- Numero di telefono: 011 19878715
- Posta certificata:tecnolink@mypec.eu
- Persona di riferimento: Antonio Cappiello
- Indirizzo email: cappiello@anticorruzioneintelligente.it

Misure di sicurezza adottate dal Responsabile esterno del trattamento dei dati

A seguito dell'utilizzo del servizio in cloud Whistleblowing Intelligente https://wb.anticorruzioneintelligente.it/
possono essere acquisiti dati relativi a persone identificate o identificabili.

COOKIES

Nessun dato personale degli utenti viene in proposito acquisito dalla piattaforma.

Non viene fatto uso di cookies per la trasmissione di informazioni di carattere personale, né vengono utilizzati c.d. cookies persistenti di alcun tipo, ovvero sistemi per il tracciamento degli utenti.
L'uso di c.d. cookies di sessione, c.d. "tecnici" (che non vengono memorizzati in modo persistente sul computer dell'utente e svaniscono con la chiusura del browser) è strettamente limitato alla trasmissione di identificativi di sessione (costituiti da numeri casuali generati dal server) necessari per consentire l'esplorazione sicura ed efficiente del servizio.
I c.d. cookies di sessione utilizzati evitano il ricorso ad altre tecniche informatiche potenzialmente pregiudizievoli per la riservatezza della navigazione degli utenti e non consentono l'acquisizione di dati personali identificativi dell'utente.

ULTERIORE RESPONSABILE DEL TRATTAMENTO

I dati personali raccolti dalla piattaforma https://wb.anticorruzioneintelligente.it/ sono trattati dalla Società:

Interzen Consulting s.r.l.,
con sede in Pescara, Strada Comunale Piana 3, cap. 65129 (P. IVA e C.F. 01446720680), in persona dell'amministratore delegato pro tempore

regolarmente nominata da Tecnolink S.r.l con atto formale come sub responsabile del trattamento dei dati personali.

SICUREZZA DEL TRATTAMENTO – PIANO DI GESTIONE DEL RISCHIO

Il responsabile indirettamente e il sub responsabile direttamente: attua le seguenti misure:

- si accerta che chiunque agisca sotto la propria autorità ed abbia accesso a dati personali, non tratti tali dati se non è stato istruito in tal senso dal responsabile stesso e vincolato contrattualmente (o ex lege) alla riservatezza/segreto
- applica le misure minime di sicurezza ict per le pubbliche amministrazioni individuate dall AGID
- applica misure tecniche di crittografia dei dati personali, dei documenti e del DB
- garantisce la riservatezza e l'integrità adottando strumenti e tecnologie di accesso mediante sistemi di autenticazione forte
- adotta mezzi che permettono di garantire la continuità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento
- adotta mezzi che permettono di garantire la capacità di ripristinare la disponibilità e l'accesso ai dati personali in caso di incidente fisico o tecnico]
- adotta delle misure tecniche per la gestione dei log a norma di legge
- luogo fisico di archiviazione dei dati: Italia

- modalità’ di conservazione dei dati, conservazione digitale

Vedi il dettaglio delle misure riportato più avanti

PERIODO DI CONSERVAZIONE

I dati personali saranno conservati sino al termine dell'incarico di erogazione del servizio di “Whistleblowing Intelligente” e comunque per un periodo di tempo non superiore ad anni 5

Dettaglio misure di sicurezza

1° LIVELLO – SISTEMI ESTERNI DI PREVENZIONE	
Scansione online delle vulnerabilità	**Nessus® Essentials: soluzione per la rilevazione delle vulnerabilità di Tenable®, Inc. Nel 2021 Tenable è stato un Software Vendor di Gartner rappresentativo della Vulnerability Assessment.**

2° LIVELLO – INFRASTRUTTURA I.T. DEL CLOUD SERVICE PROVIDER	
Service Provider	**Microsoft Azure.**
Tipologia di servizio	**Public Cloud**

cloud	
Certificazioni del cloud service provider	**Consulta la documentazione di conformità di Microsoft Azure.**
Localizzazione dei data center utilizzati	**West Europe (Netherlands)**
Livelli di sicurezza adottati dal service provider	**Operazioni eseguite da Microsoft per proteggere l’infrastruttura di Azure.**
Ridondanza dei dati del service provider	**Archiviazione con ridondanza di zona (Zone Redundancy Storage, ZRS): replica i dati archiviati in Azure in modalità sincrona su tre aree disponibili interne all’area primaria (primary region).**

3° LIVELLO – INFRASTRUTTURA I.T.	
Firewall	**Tecnolink ha adottato pfSense®, firewall riconosciuto come uno dei più potenti, sicuri ed affidabili.**
Back-up	**Procedura di back-up delle Virtual Machine**: · 1. Frequenza: ogni 4 ore. · 2. Modalità di archiviazione: ridondanza geografica GRS (GEO-REDUNDANT-STORAGE). Copia dei dati in modo sincrono tre volte all'interno di un'unica posizione fisica nell'area primaria usando l'archiviazione con ridondanza locale. Copia quindi i dati in modo asincrono in un'unica posizione fisica nell'area secondaria. All'interno dell'area secondaria i dati vengono copiati in modo sincrono tre volte usando l'archiviazione con ridondanza locale. · 3. Area Primaria: West Europe (Netherlands). · 4. Area Secondaria : North Europe (Ireland). • 5. Retention Backup: 15 giorni.
disaster recovery	**Procedura di Disaster Recovery delle Virtual Machine:** 1. Modalità: Cross Region Restore. 2. Ridondanza: geografica (Geo-Redundancy Storage, GRS). Replica dei dati archiviati in Azure in modalità sincrona su una località fisica differente (regione secondaria). 3. Localizzazione del data center utilizzato per il Disaster recovery: North Europe (Ireland).

	RTO (Recovery Time Objective, il tempo necessario per il ripristino del sistema): 2 giorni lavorativi (tempo minimo)
	RPO (Recovery Point Objective, quantità massima di dati - espressa in ore - che l'azienda perde a seguito del verificarsi di un evento disastroso, poiché non rientrati nella normale procedura ciclica di back-up): 4 ore (tempo massimo)

4° LIVELLO – COMPONENTI SOFTWARE	
Sistema operativo	Antivirus Microsoft Forefront
Server virtuale	L’accesso ai server virtuali avviene mediante una VPN ed utilizzando un profilo utente dimensionato strettamente in base alle necessità di monitoraggio e manutenzione.

5° LIVELLO – CODICE APPLICATIVO	
Sicurezza informatica di Tecnolink	Nell'ambito del processo di qualificazione del Cloud Marketplace ACN, Tecnolink ha validato i propri livelli di gestione della riservatezza e della sicurezza dei dati della soluzione

	Whistleblowing Intelligente presso lo STAR Registry (Security, Trust, Assurance, and Risk) della Cloud Security Alliance. **Visualizza la scheda di qualificazione del Marketplace ACN Cloud** Visualizza la scheda di Whistleblowing intelligente **su Cloud Security Alliance** Visualizza la scheda di Tecnolink **su Cloud Security Alliance**
Sistema di autenticazione	**Sistema proprietario. È il sistema che vincola la password di accesso del singolo utente alle seguenti regole:** **1.Scadenza alla prima autenticazione sulla piattaforma ZenShare;** **2. Lunghezza minima di 8 caratteri;** **3. Scadenza periodica ogni 3 mesi;** **4.Divieto di riutilizzo delle ultime 5 password;** **5. Vincoli sulla complessità della password (utilizzo di una lettera maiuscola/minuscola, numero, simbolo, divieto dello username);** **6. Vincoli sulla complessità della password (utilizzo di una lettera maiuscola/minuscola, numero, simbolo, divieto dello username);**

	7.Blocco dell’utente dopo 5 tentativi falliti. **Interfacciamento con sistemi esterni. Possibilità di demandare la gestione dell’accesso utenti mediante procedura di Single Sign On con altri sistemi:** **1. Microsoft (Azure Active Directory);** **2.Google (account Google);** **3. LDAP (Lightweight Directory Access Protocol);** **4.CAS (Central Authentication Service).** **5. SPID (Sistema Pubblico di Identità Digitale)**
IP filtering	**Utenti collegati. Possibilità di visualizzare tutti gli utenti autenticati (non i Segnalanti) sulla piattaforma Whistleblowing Intelligente con i seguenti dati: cognome, nome, ruolo, indirizzo IP, ultimo accesso effettuato.**

6° LIVELLO – DATI E DOCUMENTI DELLA PIATTAFORMA WHISTLEBLOWING INTELLIGENTE	
Criptaggio database e	**1.Database. Chiave di criptazione dati a sua volta criptata mediante un algoritmo per un ulteriore livello di sicurezza. Il dato resta criptato nel**

documenti	database e la sua decrittazione avviene solo quando viene visualizzato. 2. Documenti. Criptazione e decriptazione mediante chiave privata.
Protocollo HTTPS	L'HyperText Transfer Protocol Secure (over Secure Socket Layer) è un protocollo per la comunicazione su Internet che protegge integrità e riservatezza dei dati scambiati tra la Suite ZenShare e l'hardware (PC, tablet, smartphone) dell'utente che vi accede. Certificato SSL erogato da Network Solutions LLC.