# Informativa piattaforma

## Scopo e finalità

Il presente documento fornisce le informazioni relative alla piattaforma web utilizzata da Monfer S.p.A per la gestione dell''istituto del Whistleblowing così come disciplinato dal d.lgs. del 10 marzo 2023 n. 24.

## La tutela della riservatezza

L'identità del segnalante non può essere rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni.
L'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi direttamente o indirettamente tale identità, non possono essere rivelate senza il consenso espresso della stessa persona segnalante.

Restano ferme le responsabilità disciplinari e/o contrattuali previste per violazione degli appositi doveri di comportamento e per violazione delle norme sulla tutela dei dati personali.

La Monfer S.p.A. assicura la riservatezza anche della persona coinvolta e citata dal segnalante e nei confronti di eventuali facilitatori o altre persone menzionate a diverso titolo nella segnalazione.

La riservatezza del segnalante e della persona coinvolta o menzionata è garantita anche:

1. nel caso di segnalazioni effettuate in forma orale attraverso la piattaforma unificata adottata “Whistleblowing Intelligente” la quale consente di registrare segnalazioni vocali o, su richiesta della persona segnalante, di richiedere un incontro diretto con la persona autorizzata a raccogliere la segnalazione verbale
2. quando la segnalazione viene effettuata con modalità diverse da quelle istituite
3. quando la segnalazione perviene a personale interno diverso da quello autorizzato al trattamento delle segnalazioni, al quale va in ogni caso trasmessa senza ritardo.

Qualora, per ragioni istruttorie, altri soggetti debbano essere messi a conoscenza del contenuto della segnalazione e/o della documentazione ad essa allegata, i soggetti autorizzati alla gestione della segnalazione provvedono ad oscurare l’identità del segnalante e, nel limite del possibile, anche del segnalato e di eventuali altri soggetti citati ed ogni altra informazione dalla quale sia possibile risalire alla loro identità.

Ciò vale anche nei casi in cui la Monfer S.p.A. debba trasmettere la segnalazione ad altra autorità competente

Monfer S.p.A. prevede forme di responsabilità disciplinare in capo ai soggetti competenti a gestire le segnalazioni in caso di violazione dell'obbligo di riservatezza dell'identità del segnalante e degli altri soggetti la cui identità va tutelata.

## Durata di conservazione e possibilità di accesso alla segnalazione

La segnalazione sarà resa disponibile tanto al segnalante quanto al personale autorizzato per due anni. Segnalante e personale autorizzato potranno utilizzare la chat asincrona contenuta nel modulo di segnalazione della piattaforma informatica anche quando l'esame della segnalazione si è già concluso con un esito motivato.

# Obblighi di sicurezza e trattamento dei dati personali

La Società Tecnolink S.r.l. è ideatrice e proprietaria della piattaforma informatica Whistleblowing Intelligente adottata da Monfer S.p.A. in modalità Software as a Service (SaaS).

La piattaforma Whistleblowing Intelligente è registrata nel cloud marketplace dell'Autorità per la Cybersicurezza Nazionale (ACN)
https://catalogocloud.acn.gov.it/service/657

La Monfer S.p.A. è l'unico titolare del trattamento relativo ai dati inerenti alle procedure di whistleblowing.

La società Tecnolink S.r.l nella persona del suo legale rappresentante pro tempore, è stata nominata Responsabile del trattamento dei dati personali con addendum contrattuale firmato in data 04/12/2023 e disponibile presso la sede Monfer S.p.A. di Cuneo.

Monfer S.p.A., nell'ambito di quanto previsto nell'atto di nomina, verifica e controlla le modalità operative con cui il Responsabile 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.

La piattaforma Whistleblowing Intelligente consente ai soggetti interessati di trattare i dati personali secondo i principi fondamentali del già citato Regolamento UE, in particolare:

- garantire il divieto di tracciamento. Nel caso in cui l'accesso avvenga dalla rete dati interna del soggetto obbligato e sia mediato da dispositivi firewall o proxy, deve essere garantita la non tracciabilità del segnalante nel momento in cui viene stabilita la connessione con la piattaforma
- garantisce il tracciamento dell'attività del personale autorizzato nel rispetto delle garanzie a tutela del segnalante, al fine di evitare l'uso improprio di dati relativi alla segnalazione.
- evita il tracciamento di qualunque informazione che possa ricondurre all'identità o all'attività del segnalante

Per conoscere nel dettaglio le misure tecniche adottate dal fornitore consulta l'allegato 3 del presente documento.

Monfer S.p.A. assegna specifici compiti e funzioni connessi al trattamento di dati personali in relazione alle procedure di Whistleblowing. Tali compiti specifici sono attribuiti a persone fisiche, espressamente designate, che operano sotto l'autorità del titolare del trattamento.

Qualsiasi scambio e trasmissione di informazioni inerente le segnalazioni che comportano un trattamento di dati personali, deve avvenire in conformità al regolamento UE 2018/1725.

## Diritto degli interessati

La persona coinvolta o la persona menzionata nella segnalazione, con riferimento ai propri dati personali trattati nell'ambito della segnalazione, divulgazione pubblica o denuncia, non possono esercitare i diritti che normalmente il GDPR riconosce agli interessati (il diritto di accesso ai dati personali, il diritto a rettificarli, il diritto di ottenerne la cancellazione o cosiddetto diritto all'oblio, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati personali e quello di opposizione al trattamento).

Dall'esercizio di tali diritti potrebbe derivare un pregiudizio effettivo e concreto alla tutela della riservatezza dell'identità della persona segnalante.
In tali casi, dunque, al soggetto segnalato o alla persona menzionata nella segnalazione è preclusa la possibilità, laddove ritengano che il trattamento che li riguarda violi suddetti diritti, di rivolgersi al titolare del trattamento e, in assenza di risposta da parte di quest'ultimo, di proporre reclamo al Garante della protezione dei dati personali.
Ulteriori informazioni su questo punto sono reperibili sulla specifica informativa sul trattamento dei dati personali reperibile al seguente link (https://monfer.net/segnalazioni-whistleblowing/)

# Le persone autorizzate al trattamento delle Segnalazioni

La responsabilità della corretta applicazione della disciplina sul Whistleblowing ricade sul Responsabile della gestione delle segnalazioni designato da Monfer S.p.A.

Il Responsabile può avvalersi della collaborazione di personale interno adeguamento formato.

In particolare, i soggetti che gestiscono le segnalazioni devono:

- essere autorizzati al trattamento dei dati personali e quindi essere destinatari di una specifica formazione in materia di privacy sul trattamento dei dati personali
- assicurare indipendenza e imparzialità
- ricevere un'adeguata formazione professionale sulla disciplina del whistleblowing, anche con riferimento a casi concreti

# Segnalazioni acquisite attraverso la piattaforma Whistleblowing Intelligente

La Monfer S.p.A. ha istituito un canale integrato interno denominato “Whistleblowing Intelligente” per la ricezione e gestione delle segnalazioni di violazioni di disposizioni normative nazionali o dell’Unione europea che ledono l’interesse pubblico o l’integrità dell’amministrazione pubblica.

La piattaforma garantisce, tramite il ricorso a strumenti di crittografia, la riservatezza dell’identità della persona segnalante, della persona coinvolta e della persona menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

Whistleblowing Intelligente utilizza, sia per le segnalazioni sia per le eventuali comunicazioni successive, un protocollo di crittografia che meglio garantisce sicurezza e confidenzialità tecnologica del processo di segnalazione.

Attraverso il protocollo di crittografia, i dati del segnalante vengono segregati in una sezione dedicata della piattaforma, inaccessibile, in prima istanza, anche al Responsabile del trattamento delle segnalazioni e agli eventuali soggetti autorizzati.

Nella piattaforma informatica sono riportati i link all'informativa specifica sul trattamento dei dati personali (https://monfer.net/segnalazioni-whistleblowing/) e al presente atto organizzativo (https://monfer.net/segnalazioni-whistleblowing/).

## I soggetti che operano nel canale di segnalazione

Nella piattaforma sono autorizzati ad operare i seguenti soggetti:

- Responsabile della gestione delle segnalazioni (accesso tramite login)
- Eventuali collaboratori del Responsabile (tramite login ma con accesso limitato alle sole segnalazioni assegnate loro dal Responsabile)
- Segnalante (senza necessità di effettuare login) il quale può fare segnalazioni e accedervi successivamente, ma esclusivamente attraverso il codice univoco di segnalazione rilasciato dal sistema al momento in cui la segnalazione è stata effettuata.

## Fare una segnalazione

Nella home page del sito www.monfer.net è inserito il link ad una pagina di presentazione del servizio (https://monfer.net/segnalazioni-whistleblowing/) con la possibilità di scegliere l'accesso al canale di segnalazione con identità certificata attraverso lo SPID (preferibile) oppure con identità auto dichiarata non obbligatoria.

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

È necessario che la segnalazione sia il più possibile circostanziata al fine di consentire la delibazione dei fatti da parte dei soggetti competenti a ricevere e gestire le segnalazioni, In particolare è necessario risultino chiare:

- le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione
- la descrizione del fatto
- le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati

È utile anche allegare documenti e file multimediali che possano fornire elementi di fondatezza dei fatti oggetto di segnalazione, nonché fornire l'indicazione di altri soggetti potenzialmente a conoscenza dei fatti.

Al segnalante si richiede un comportamento collaborativo tenendo costantemente aggiornata la Monfer S.p.A. in ordine all'evoluzione della propria segnalazione secondo le modalità descritte più avanti.

## Il Codice univoco di segnalazione

All'invio della segnalazione, la piattaforma presenta al segnalante una videata con il codice univoco di segnalazione il quale deve essere acquisito e conservato per ricollegarsi alla piattaforma nei momenti successivi, in modo tale da poter:

- integrare/aggiornare in un secondo momento quanto riportato inizialmente nel modulo di segnalazione
- rispondere ad eventuali richieste di chiarimenti/approfondimenti da parte dei soggetti autorizzati
- verificare l'avanzamento dell'iter di gestione della segnalazione
- esprimere o negare il consenso a rivelare la propria identità nell'ambito del procedimento disciplinare originatosi dalla segnalazione

Se il segnalante fornisce all'interno della segnalazione un indirizzo di posta elettronica, la piattaforma gli invierà le notifiche con un link attraverso il quale potrà accedere alla segnalazione senza dover digitare il codice univoco di segnalazione.

Monfer S.p.A. non è nella condizione di poter fornire il codice univoco di segnalazione in caso di smarrimento e neanche di generarne uno nuovo.

## Ricezione della segnalazione

Al momento della ricezione della segnalazione, il sistema registra la data e l'ora di acquisizione; assegna alla segnalazione un numero progressivo e un ID di segnalazione.

Nessuno di questi dati può essere manipolato e nessuna segnalazione può essere cancellata prima della scadenza del tempo di archiviazione previsto in anni 2.

Contemporaneamente, la piattaforma informa via email dell'avvenuta ricezione della segnalazione il segnalante (se ha inserito un indirizzo di posta elettronica nella segnalazione) e il Responsabile.

Il Responsabile è l'unico soggetto a cui sono dati i permessi di prendere in carico la segnalazione entro 7 giorni dalla data di ricezione.

Il Responsabile prende in carico la segnalazione entrando nella piattaforma ed aprendola. Anche in questo caso la piattaforma aggiorna immediatamente il segnalante dell'avvenuta presa in carico.

Dal momento in cui la segnalazione è stata presa in carico, decorrono i tempi per la chiusura della segnalazione (90 gg)

## Esame preliminare

L'esame preliminare ha lo scopo di accertare da un lato se esistono i presupposti per accordare le tutele al segnalante e, dall'altro, se la segnalazione contiene elementi meritevoli di essere approfonditi in fase istruttoria.

Il Responsabile o il collaboratore da questi designato all'interno della piattaforma, valuta la sussistenza dei requisiti di ammissibilità.
La segnalazione è considerata inammissibile e viene archiviata in via diretta per almeno uno dei seguenti motivi:

- manifesta infondatezza per l'assenza di elementi di fatto riconducibili alle violazioni tipizzate nell'art. 2, co. 1, lett. a) e a giustificare ulteriori accertamenti
- manifesta incompetenza di Monfer S.p.A. sulle questioni segnalate
- 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

Nei casi in cui quanto segnalato non sia adeguatamente circostanziato, il soggetto autorizzato a trattare la segnalazione può chiedere al whistleblower, all'interno della piattaforma, elementi integrativi e di chiarimento/precisazione.

Il sistema automaticamente tiene traccia delle interlocuzioni con la persona segnalante e fornisce informazioni sullo stato di avanzamento dell'iter di esame della segnalazione

## Fase istruttoria

Anche durante la fase istruttoria potranno essere sottoposte al segnalante domande, richieste di integrazioni, chiarimenti e tutto quanto può servire a delineare correttamente i contorni della vicenda segnalata.

La comunicazione con il segnalante avverrà unicamente all'interno della piattaforma Whistleblowing Intelligente. Nessun altro mezzo sarà utilizzato.
Le richieste di integrazioni/chiarimenti interrompono il conteggio dei tempi di esame della segnalazione. Detti tempi riprendono in automatico alla risposta da parte del segnalante.

La piattaforma consente al soggetto designato alla trattazione della segnalazione di tenere un diario in cui segnare le date e il tipo di attività istruttorie svolte, come ad esempio: l'acquisizione di documentazione; interlocuzioni e altre attività utili al solo fine di accertare l'attendibilità della segnalazione.

## Verbale delle risultanze istruttorie e chiusura della segnalazione

Il verbale delle risultanze istruttorie sarà scritto direttamente all'interno della piattaforma, evitando così upload e download di file in modo tale da meglio garantire la protezione e riservatezza delle informazioni ivi contenute.

L'intero iter di esame e verifica della segnalazione si dovrà concludere entro 90 giorni dalla data di presa in carico, fatte salve le interruzioni in attesa delle risposte da parte del segnalante quando gli vengono inviati messaggi con la richiesta di ulteriori informazioni/precisazioni.

I possibili esiti dell'esame della segnalazione sono i seguenti:

- inammissibile
- improcedibile
- archiviata per infondatezza
- inviata all'Ufficio Provvedimenti Disciplinari (UPD)
- inviata all'ANAC
- inviata alla Corte dei conti
- Inviata all'Autorità giudiziaria

Al momento della chiusura, il soggetto autorizzato ad esaminare la segnalazione scrive anche una breve nota sulle motivazioni riguardo all'esito.
La piattaforma comunicherà prontamente all'indirizzo di posta elettronica rilasciato dal segnalante, esito e motivazione.

Nell'invio ai diversi destinatari, il Responsabile della gestione delle segnalazioni avrà cura di mantenere segreta l'identità del segnalante e di non rivelare nessun fatto o circostanza da cui si possa risalire all'identità del segnalante.
Inoltre, nelle comunicazioni con i diversi interlocutori, dovrà sempre essere indicato che si tratta di segnalazione di Whistleblowing da trattare nei limiti indicati nel decreto 24/2023

### Il Custode dell'identità digitale del segnalante e l'accesso ai dati

Il Responsabile svolge anche il ruolo di "Custode dell'identità" del segnalante e ha sempre la possibilità di accedere ai suoi dati identificativi per gli usi consentiti o richiesti dalla legge.

L'accesso ai dati identificativi del segnalante è motivato e la motivazione viene registrata all'interno della piattaforma informatica.
Il Segnalante riceve avviso delle motivazioni per le quali i suoi dati identificativi sono stati messi in chiaro.

## Segnalazioni raccolte via registrazione vocale

Il canale integrato Whistleblowing Intelligente, consente al segnalante di effettuare una registrazione vocale per raccontare la segnalazione in un limite di tempo di venti minuti.

La segnalazione così raccolta sarà gestita allo stesso modo della segnalazione acquisita tramite la compilazione dell'apposito form predisposto sul canale integrato Whistleblowing Intelligente.

## Segnalazioni raccolte tramite Incontri diretti

Accedendo ai link predisposti da Monfer S.p.A. sul proprio sito, il segnalante potrà scegliere un modulo per la richiesta di incontro al fine di rilasciare verbalmente una segnalazione di condotte illecite.

IL Responsabile riceve avviso di richiesta di incontro e accede alla piattaforma per comunicare data, ora e luogo dell'incontro. La piattaforma si incaricherà di inviare al segnalante i dati per l'incontro.
Durante l'incontro - previa presentazione dell'informativa del trattamento dei dati personali e delle informazioni necessarie per reperire il testo completo di tale informativa - il Responsabile acquisisce il racconto verbale del segnalante o tramite registrazione vocale oppure verbalizzando le dichiarazioni del segnalante.
La registrazione vocale dell'incontro o, in alternativa, il verbale sottoscritto dal segnalante, saranno aggiunte alla richiesta di incontro andando così a configurare un terzo tipo di segnalazione gestito dal canale unificato di segnalazione utilizzato da Monfer S.p.A.
A questo punto la segnalazione sarà gestita e trattata come le segnalazioni del tipo precedentemente illustrate.

# Allegato 1

## 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 PRIVACY

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: UE
- 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". A cura del Responsabile della gestione delle segnalazioni, saranno eliminate le segnalazioni che eccedono il tempo di conservazione indicato in fase di configurazione

Durante il periodo contrattuale e anche per il mese successivo, il cliente ha la possibilità di scaricare ogni singola segnalazione e/o l'insieme delle segnalazioni in forma tabellare per gli usi che ritiene più opportuni.
Allo scadere del contratto, decorsi 30 giorni nei quali il cliente non ha manifestato formalmente la volontà di rinnovare il servizio, Tecnolink cancellerà definitivamente i dati trattati.

# 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 cloud** | **Public 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** | **PfSense®, firewall riconosciuto come uno dei più potenti, sicuri ed affidabili.** |

| | |
|---|---|
| **Back-up** | **Procedura di back-up delle Virtual Machine**:<br>● 1. Frequenza: ogni 4 ore.<br>● 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.<br>● 3. Area Primaria: West Europe (Netherlands).<br>● 4. Area Secondaria : North Europe (Ireland).<br>● 5. Retention Backup: 15 giorni. |
| **disaster recovery** | **Procedura di Disaster Recovery delle Virtual Machine:**<br>1. Modalità: Cross Region Restore.<br>2. Ridondanza: geografica (Geo-Redundancy Storage, GRS). Replica dei dati archiviati in Azure in modalità sincrona su una località fisica differente (regione secondaria).<br>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 del produttore | Nell'ambito del processo di qualificazione del Cloud Marketplace ACN, il produttore 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.<br><br>Visualizza la scheda di qualificazione del Marketplace ACN Cloud<br><br>Visualizza la scheda di Whistleblowing intelligente su Cloud Security Alliance<br><br>Visualizza la scheda del produttore su Cloud Security Alliance |
| Sistema di autenticazione | Sistema proprietario. È il sistema che vincola la password di accesso del singolo utente<br><br>Interfacciamento con sistemi esterni. Possibilità di demandare la gestione dell'accesso utenti mediante procedura di Single Sign On con altri sistemi:<br><br>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 documenti** | **1. Database. Chiave di criptazione dati a sua volta criptata mediante un algoritmo per un ulteriore livello di sicurezza. Il dato resta criptato nel database e la sua decrittazione avviene solo quando viene visualizzato.**<br><br>**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 piattaforma e l'hardware (PC, tablet, smartphone) dell'utente che vi accede. Certificato SSL erogato da Network Solutions LLC.** |