Lombardi

ATTO ORGANIZZATIVO DI ATTUAZIONE DELLA DISCIPLINA IN MATERIA DI *WHISTLEBLOWING*

(D.LGS. DEL 10.3.2023 N. 24)

Adottato con delibera del CdA
del 15/12/2023

Lombardi Ingegneria S.r.l. – Socio Unico
Via Giotto 36, IT-20145 Milano
Telefono +39 02 583 03 324, Fax +39 02 583 03 190
milano@lombardi.group, www.lombardi.group

Unità locale Roma
Via XX Settembre 98/G, IT-00185 Roma, Italy

Unità locale Torino
Via R. Montecuccoli 9, IT-10121 Torino, Italy
torino@lombardi.group, www.lombardi.group

Certificato SGS ISO 9001:2015 | CH97/0470
Certificato SGS ISO 14001:2015 | CH16/0455
Certificato SGS ISO 45001:2018 | CH21/0629
C.F./P.I.: N°12151290157, Reg. Imprese di Milano N° 12151290157
R.E.A. di Milano N° 1530711, Capitale sociale € 110.000,00

Lombardi Ingegneria S.r.l. – Socio Unico
Via Giotto 36, IT-20145 Milano
Telefono +39 02 583 03 324, Fax +39 02 583 03 190
milano@lombardi.group, www.lombardi.group

Unità locale Roma
Via XX Settembre 98/G, IT-00185 Roma, Italy

Unità locale Torino
Via R. Montecuccoli 9, IT-10121 Torino, Italy
torino@lombardi.group, www.lombardi.group

Certificato SGS ISO 9001:2015 | CH97/0470
Certificato SGS ISO 14001:2015 | CH16/0455
Certificato SGS ISO 45001:2018 | CH21/0629
C.F./P.I.: N°12151290157, Reg. Imprese di Milano N° 12151290157
R.E.A. di Milano N° 1530711, Capitale sociale € 110.000,00

1. PREMESSA

1.1 Whistleblowing: fonte normativa e natura dell'istituto

Il Decreto Legislativo 10 marzo 2023 n. 24 (d'ora in avanti anche Decreto *Whistleblowing* o Decreto), entrato in vigore il 30 marzo 2023, dà attuazione alla direttiva UE 2019/1937, avente ad oggetto la protezione dei cd. *Whistleblowers* (o "informatori", nella traduzione italiana del testo), ossia delle persone che segnalano, a seconda dei casi e come si vedrà meglio *infra*, 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.

Con tale direttiva è stato introdotto, per tutti gli Stati membri, un vero e proprio diritto alla segnalazione. Il D.Lgs. n. 24/2023 raccoglie in un unico testo normativo l'intera disciplina dei canali di segnalazione, interni ed esterni, nonché delle altre forme di segnalazione e del sistema di tutele riconosciute ai segnalanti (e in favore degli altri soggetti espressamente individuati dal Legislatore), sia del settore pubblico che privato. Ne deriva una disciplina organica e uniforme finalizzata ad una maggiore tutela del *Whistleblower*, di modo che quest'ultimo disponga degli strumenti per poter cooperare nell'emersione delle eventuali violazioni rilevanti, venendo edotto, sin dal principio, dei diritti e dei doveri la cui osservanza è fondamentale per assolvere alla funzione della normativa stessa.

Considerato, inoltre, che la Società è intenzionata a dotarsi di un Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. n. 231/2001 (d'ora in avanti anche MOGC 231), avendo già conferito apposito incarico consulenziale, dal momento della sua formale adozione anche le violazioni rilevanti ai sensi della predetta normativa ovvero le violazioni di procedure di cui il Modello stesso si compone potranno costituire oggetto di segnalazione ai fini del presente Atto Organizzativo e, ove ricorrano le condizioni previste dal D.Lgs. n. 24/2023, saranno coperte dalle medesime garanzie e tutele.

L'attuale disciplina persegue la finalità di favorire l'emersione e la prevenzione di rischi e situazioni pregiudizievoli per i soggetti pubblici e privati interessati, nonché – di riflesso – per l'interesse pubblico collettivo.

Tale obiettivo viene perseguito stimolando la cooperazione di quanti gravitano o hanno gravitato nell'ambito del contesto lavorativo pubblico o privato, attraverso il rafforzamento del sistema di protezione previsto a loro tutela, sia sul piano della riservatezza che in caso di ritorsioni.

1.2 Scopo del documento e sintesi dei contenuti

La Società è impegnata a promuovere una cultura aziendale caratterizzata da comportamenti corretti e da un efficiente sistema di *corporate governance*.
La Società opera nel pieno rispetto di tutte le leggi e regolamenti sovranazionali, nazionali e locali applicabili, richiedendo la medesima accortezza a tutto il suo personale e ai soggetti terzi con i quali interagisce nell'esercizio della propria attività.

Per tali ragioni, la Società riconosce l'importanza di definire nel presente Atto Organizzativo le procedure che regolano l'intero processo di invio, ricezione, analisi e gestione delle segnalazioni delle violazioni rilevanti ai fini del D.Lgs. n. 24/2023, con l'obiettivo di promuovere un ambiente aziendale in cui le funzioni apicali, i dipendenti e le terze parti dispongano degli strumenti per valutare la rilevanza delle condotte riscontrate e, laddove ne ricorrano i presupposti, si sentano a proprio agio nell'inoltrare simili comunicazioni, ritenendo che dalla collaborazione di tutti i soggetti coinvolti nelle dinamiche societarie possano raggiungersi i più elevati standard di efficienza e legalità.

Dal momento della formale adozione del Modello di Organizzazione, Gestione e Controllo *ex* D.Lgs. n. 231/2001, inoltre, il presente Atto Organizzativo ne diverrà parte integrante.

1.3 Destinatari

I destinatari delle disposizioni contenute nel presente Atto Organizzativo sono da individuare nei seguenti soggetti:

- i soci;
- le persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della

Società e che esercitano anche di fatto la gestione e il controllo della stessa;

- i dipendenti;
- i partner, i clienti, i fornitori, i consulenti, i collaboratori (anche volontari e/o tirocinanti) e, più in generale, chiunque sia in relazione d'interessi con la Società (cd. "terze parti").

Per segnalante, ai sensi del Decreto *Whistleblowing*, s'intende "*la persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo*".

1.4 Oggetto della segnalazione

Per segnalazione s'intende la comunicazione scritta od orale di informazioni sulle violazioni rilevanti ai fini del Decreto *Whistleblowing*, avvenute nello svolgimento dell'attività lavorativa o che abbiano un impatto, diretto o indiretto, sulla stessa, che arrechino o che possano arrecare danno o pregiudizio alla Società, ai suoi dipendenti o a soggetti terzi.

Possono essere oggetto di segnalazione le informazioni, compresi i fondati sospetti, sulle:

1. violazioni del diritto dell'UE e di tutte le disposizioni nazionali di recepimento nelle materie di cui all'allegato 1 del D.Lgs. n. 24/2023. Si tratta, in particolare, dei seguenti settori: contratti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali; sicurezza delle reti e dei sistemi informativi;
2. atti od omissioni che ledono gli interessi finanziari dell'UE (art. 325 del Trattato sul funzionamento dell'UE, lotta contro la frode e le attività illegali che ledono gli interessi finanziari dell'UE), come individuati nei regolamenti, direttive, decisioni, raccomandazioni e pareri dell'UE. Si pensi, ad esempio, alle frodi, alla corruzione e a qualsiasi altra attività illegale connessa alle spese dell'UE;
3. atti od omissioni riguardanti il mercato interno, che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali (art. 26, pr. 2, del Trattato sul funzionamento dell'UE). Sono ricomprese le violazioni delle norme dell'UE in materia di concorrenza e di aiuti di Stato, di imposta sulle società e i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società;
4. atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni dell'UE nei settori indicati ai punti precedenti;

5. condotte illecite rilevanti ai sensi del D.Lgs. n. 231/2001 e violazioni del MOGC 231 (per ciò che concerne la Società, solo a far data dal momento della sua formale adozione e previo invio di apposita informativa, da effettuare nei confronti di tutti i soggetti destinatari).

Le predette violazioni possono essere integrate da qualsiasi provvedimento, comportamento, atto od omissione posto in essere nello svolgimento dell'attività lavorativa o che abbiano un impatto, diretto o indiretto, sulla stessa, che arrechino o che possano arrecare danno o pregiudizio alla Società, ai suoi dipendenti o a soggetti terzi.

Le informazioni sulle violazioni possono riguardare anche le violazioni non ancora commesse che il *Whistleblower*, ragionevolmente, ritiene potrebbero esserlo sulla base di elementi concreti, precisi e concordanti[1], oltreché le condotte finalizzate ad occultare le violazioni stesse.

Le segnalazioni possono essere effettuate non solo quando è in corso uno dei rapporti giuridici indicati nel paragrafo precedente, ma, ai sensi dell'art. 3, comma 4, del D.Lgs. n. 24/2023, anche:

a) quando il rapporto giuridico non è ancora iniziato, se le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali;
b) durante il periodo di prova;
c) successivamente allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite prima della fine del rapporto stesso.

Non costituiscono, invece, segnalazione rilevante ai fini del Decreto *Whistleblowing* e, di conseguenza, non si applicano le garanzie e le tutele ivi previste, le contestazioni/rivendicazioni/richieste/ comunicazioni:

1. legate ad un interesse personale del segnalante, che attengono esclusivamente ai rapporti individuali di lavoro (ferma tale precisazione, va evidenziato che i motivi che inducono il segnalante ad effettuare la segnalazione non assumono rilievo ai fini della relativa trattazione, né in ordine all'applicazione del sistema di tutele e garanzie previste dal Decreto);
2. in materia di difesa e sicurezza nazionale;
3. relative a violazioni riguardanti alcuni settori speciali, già disciplinati in via obbligatoria dagli atti dell'UE o dalle relative disposizioni nazionali di recepimento, nonché direttamente dagli

[1] Tali elementi possono essere costituiti da irregolarità e/o anomalie (cd. indici sintomatici) che il segnalante ritiene possano dar luogo ad una delle violazioni previste dal Decreto.

atti nazionali, indicati nella parte II dell'allegato al D.Lgs. n. 24/2023, (i.e. servizi finanziari, prevenzione riciclaggio, terrorismo, sicurezza nei trasporti, tutela dell'ambiente);

4. aventi per oggetto notizie palesemente prive di fondamento, nonché già totalmente di dominio pubblico oppure qualora si tratti di mere indiscrezioni o voci di corridoio.

Le segnalazioni, in ogni caso, devono essere effettuate in buona fede, con spirito di responsabilità ed essere necessariamente circostanziate con informazioni precise e sufficienti all'avvio delle relative verifiche.

Lombardi Ingegneria S.r.l. – Socio Unico
Via Giotto 36, IT-20145 Milano
Telefono +39 02 583 03 324, Fax +39 02 583 03 190
milano@lombardi.group, www.lombardi.group

Unità locale Roma
Via XX Settembre 98/G, IT-00185 Roma, Italy

Unità locale Torino
Via R. Montecuccoli 9, IT-10121 Torino, Italy
torino@lombardi.group, www.lombardi.group

Certificato SGS ISO 9001:2015 | CH97/0470
Certificato SGS ISO 14001:2015 | CH16/0455
Certificato SGS ISO 45001:2018 | CH21/0629
C.F./P.I.: N°12151290157, Reg. Imprese di Milano N° 12151290157
R.E.A. di Milano N° 1530711, Capitale sociale € 110.000,00

2. CANALI DI SEGNALAZIONE

2.1 Canali di segnalazione interna

I canali di segnalazione interna costituiscono lo strumento privilegiato per la comunicazione delle informazioni sulle eventuali violazioni rilevanti, in quanto più prossimi all'origine delle questioni oggetto di segnalazione.

In conformità alle disposizioni del Decreto *Whistleblowing* e alle Linee Guida emanate sul tema da ANAC, la Società ha attivato e messo a disposizione dei soggetti destinatari un canale interno informatico per la trasmissione delle segnalazioni.

Il canale informatico è costituito da un portale web dedicato, accessibile all'indirizzo https://lombardigroup.wbisweb.it (cd. Portale *Whistleblowing*, di seguito anche solo Portale), gestito dalla società ISWEB S.p.A., che ne ha certificato la conformità sul piano tecnico e normativo ed è stata designata, in relazione all'attività affidatagli, come Responsabile del trattamento dei dati personali (**all. 1a-1b-1c**).

Accedendo al Portale, il segnalante verrà brevemente e nuovamente informato in merito alle caratteristiche di tale strumento.

Cliccando sul pulsante "*Invia una segnalazione*" – previa lettura e accettazione delle informative concernenti la finalità della disciplina normativa di riferimento e il trattamento dei dati personali – il segnalante potrà effettuare la segnalazione attraverso una delle modalità di seguito riportate:

- comunicazione in forma scritta, mediante compilazione del modulo attraverso il quale verrà richiesta l'indicazione delle circostanze rilevanti ai fini della compiuta descrizione della violazione segnalata (i.e., relazione del segnalante, tipologia di condotta segnalata, contesto spazio-temporale, durata della condotta, soggetti coinvolti a vario titolo, descrizione dei fatti oltreché ogni altra informazione ritenuta utile a consentire la verifica della segnalazione, inclusa l'indicazione di eventuali ulteriori soggetti preventivamente informati in merito ai medesimi fatti, come Autorità e/o Istituzioni. Per un'analisi più approfondita dei contenuti del modulo, si rinvia al form allegato, **all. 2**);

- comunicazione in forma orale, mediante caricamento sul Portale di un file audio contenente la compiuta descrizione della violazione segnalata. Tale operazione potrà essere materialmente eseguita – previa compilazione del modulo di cui sopra (cfr. **all. 2**) – attraverso l'utilizzo del pulsante "*carica*", disponibile all'interno della sezione del Portale denominata "*allegati*" (tale sezione potrà essere utilizzata anche nell'ambito della comunicazione scritta della violazione, al fine di fornire specifiche evidenze documentali, di qualsiasi formato e tipologia esse siano, a supporto dei fatti segnalati). Quanto al contenuto della comunicazione orale registrata nell'apposito file audio, laddove la compilazione del modulo presente nelle sezioni iniziali del Portale dovesse avvenire in forma riassuntiva, incompleta e/o tale da non recare l'indicazione delle informazioni espressamente richieste, si invita il segnalante a fornire all'interno del file audio stesso tutti i dati informativi richiamati all'interno del modulo, onde poter assicurare la compiuta identificazione della violazione segnalata e dei soggetti a vario titolo coinvolti;
- richiesta di incontro con il Responsabile della gestione del canale di segnalazione interna (di seguito, anche solo Responsabile della Gestione o Responsabile) per poter comunicare in quella sede ed in forma orale la segnalazione rilevata: qualora il segnalante decida di optare per tale modalità di segnalazione, sarà necessario comunque compilare le sezioni del modulo allegato individuate dal Portale come obbligatorie (cfr. **all. 2**) e accettare i termini di servizio meglio precisati *infra*, sino al completamento dell'iter di invio della segnalazione, inserendo la seguente frase nella sezione denominata "*Descrizione dei fatti*": "*E' mia intenzione chiedere al Responsabile della Gestione del canale di segnalazione interna di fissare, entro un termine ragionevole, un incontro di persona, al fine di comunicare oralmente la violazione in materia di Whistleblowing di cui sono venuto a conoscenza nello svolgimento della mia attività lavorativa*" (qualora il segnalante dovesse optare per una delle prime due modalità di trasmissione della segnalazione, successivamente all'invio di quest'ultima, egli potrebbe comunque chiedere la fissazione di un incontro di persona al Responsabile della Gestione, secondo le modalità di seguito meglio specificate).

Indipendentemente dalla modalità di invio della segnalazione prescelta dal segnalante, seguendo gli step operativi previsti dal Portale, il segnalante accederà alla sezione denominata "*identità*", al cui interno egli potrà decidere se inserire le proprie generalità oppure proseguire nella procedura di

compilazione e invio della segnalazione in forma anonima (per segnalazione anonima, s'intende, dunque, la segnalazione da cui non è possibile ricavare l'identità del segnalante).

Nel primo caso, tramite gli strumenti di crittografia di cui il Portale è dotato, l'identità del segnalante sarà resa nota soltanto al Responsabile della Gestione, il quale – conformemente al Decreto *Whistleblowing* – avrà l'obbligo di garantirne la riservatezza e potrà rivelarla soltanto qualora ciò sia assolutamente necessario e previo consenso espresso del segnalante ovvero nell'ipotesi di coinvolgimento delle competenti Autorità e dietro loro esplicita richiesta.

Nel secondo caso, premesso che la scelta di mantenere l'anonimato potrà eventualmente essere modificata dal segnalante in un secondo momento, attraverso le funzioni di cui si compone il Portale stesso, prima fra tutti la cd. "chat" (sezione denominata "*commenti*") che, come si dirà, consentirà, successivamente all'invio della segnalazione, lo scambio di informazioni tra il segnalante e il Responsabile della Gestione mediante servizio di messaggistica, la segnalazione potrà comunque essere inviata e la stessa, unitamente all'eventuale documentazione allegata, verrà archiviata e gestita dal Responsabile designato dalla Società, purché adeguatamente circostanziata e idonea a consentire lo svolgimento da parte di quest'ultimo del necessario procedimento di verifica.

La Società, infatti, sebbene la normativa prescriva un obbligo di riservatezza e non di anonimato, al fine di favorire con tutti i mezzi a propria disposizione lo spirito di cooperazione postulato dal Decreto *Whistleblowing* e verificare in concreto la sussistenza di ogni violazione ipoteticamente avvenuta nel proprio contesto lavorativo o in un ambito comunque ad esso collegato, con il presente Atto Organizzativo dispone che anche le eventuali segnalazioni anonime, purché adeguatamente circostanziate, vengano trattate alla stregua delle segnalazioni ordinarie e, dunque, sottoposte al medesimo procedimento di verifica, ricordando al tempo stesso al segnalante i doveri e le responsabilità che il Legislatore pone a suo carico in merito alla veridicità delle informazioni su cui si fonda la segnalazione stessa.

Superata la sezione "*identità*", il Portale consentirà al segnalante di accedere all'area denominata "*allegati*", al cui interno potranno essere caricate le evidenze documentali ritenute d'interesse al fine di riscontrare uno o più aspetti della violazione oggetto di segnalazione. Tramite il pulsante "*carica*", il segnalante potrà allegare i documenti e/o i file multimediali che riterrà d'interesse ai fini della

valutazione della fondatezza della violazione segnalata (l'inserimento degli allegati è facoltativo, ma fortemente consigliato nel caso in cui il segnalante disponga di tali evidenze, al fine di agevolare il procedimento di verifica affidato al Responsabile della Gestione). In caso di comunicazione orale, attraverso tale funzione del Portale il segnalante potrà caricare il file audio contenente la registrazione della propria segnalazione, attenendosi alle indicazioni fornite in precedenza.

All'esito dell'eventuale inserimento di allegati, il Portale condurrà il segnalante in una nuova sezione denominata "*ulteriori informazioni*", al cui interno, rispondendo ai quesiti di cui al modulo (cfr. **all. 2**), lo stesso potrà fornire maggiori precisazioni in merito alla segnalazione, inclusa l'eventuale indicazione del cd. "facilitatore", colui o colei che, operando all'interno del medesimo contesto lavorativo del segnalante, lo ha assistito nella segnalazione della violazione (soggetto, al quale, come si dirà, sono estese specifiche tutele).

Completata anche tale sezione, il segnalante accederà all'ultimo step operativo previsto dal Portale, attraverso il quale – previa lettura e accettazione dei termini di servizio, di cui il presente Atto Organizzativo e l'informativa privacy ad esso collegata costituiscono parte integrante – potrà procedere alla trasmissione della segnalazione cliccando il pulsante "*invia*".

Così facendo, la procedura di segnalazione verrà completata mediante l'invio del suo contenuto esclusivamente al Responsabile della Gestione e il Portale elaborerà un codice identificativo univoco progressivo denominato "*key code*".

Tale codice dovrà essere custodito e conservato a cura del segnalante, l'unico soggetto che ne verrà materialmente a conoscenza, e gli consentirà, una volta tornato all'indirizzo del Portale (https://lombardigroup.wbisweb.it) e inserito nella sezione "*Hai già effettuato una segnalazione? Inserisci la tua ricevuta*", di accedere all'area della propria segnalazione, consultarne lo stato di gestione e interagire, attraverso la cd. "chat" con il Responsabile della Gestione (anche mediante integrazioni informative e/o documentali oppure chiedendo un apposito incontro al Responsabile per poter provvedere in tal senso. Allo stesso modo, il Responsabile della Gestione potrà utilizzare tale strumento con le medesime finalità).

In caso di smarrimento, il "*key code*" non potrà essere in alcun modo recuperato. In tale ipotesi, il segnalante – per poter continuare ad essere aggiornato sullo stato di gestione della segnalazione o anche solo per poter effettuare una qualsiasi integrazione – dovrà iniziare una nuova procedura di segnalazione rispondendo in maniera affermativa al quesito "*Hai già effettuato la segnalazione ma hai perso il tuo key code?*", presente all'inizio della sezione denominata "*segnalazione*", e, nei campi informativi successivi, dovrà inserire tutti i riferimenti necessari affinché il Responsabile della Gestione possa associare la nuova segnalazione a quella ricevuta in precedenza.

2.2 Gestione delle segnalazioni interne

La Società ha affidato la gestione del canale di segnalazione interna esclusivamente ad un soggetto esterno, autonomo ed indipendente rispetto alla Società, il quale – in virtù di specifiche e comprovate competenze professionali – è stato formalmente investito dell'incarico di Responsabile della Gestione del canale di segnalazione interna e, ai fini privacy, del ruolo di Responsabile del trattamento dei dati oggetto di segnalazione.

Il predetto Responsabile sarà l'unico soggetto titolato ad accedere al contenuto delle segnalazioni inviate tramite il canale di segnalazione interna, attraverso la sezione a lui riservata del Portale *Whistleblowing*, mediante l'impiego di credenziali di autenticazione ad uso esclusivo (in caso di successiva individuazione di altro Responsabile, verrà garantita la modifica delle credenziali di accesso al Portale).

Al momento dell'invio di una segnalazione tramite Portale o di aggiornamento di una segnalazione già inviata attraverso il medesimo strumento telematico, il Portale elaborerà in automatico una notifica, priva di contenuti specifici e/o qualsivoglia dato inerente la segnalazione, che verrà trasmessa alla casella e-mail indicata dal Responsabile della Gestione e dallo stesso utilizzata in via esclusiva, affinché egli possa accedere alla propria area riservata del Portale, prendere contezza del contenuto della segnalazione e adempiere alle prescrizioni previste dal Decreto (in caso di successiva individuazione di altro Responsabile, verrà garantita la modifica della casella e-mail cui il Portale invierà le predette notifiche).

Tutte le segnalazioni saranno gestite dal Responsabile della Gestione in maniera equa ed imparziale, con la massima attenzione e nella piena osservanza di tutte le prescrizioni, gli adempimenti tecnico-operativi, le garanzie e le tutele previste dal Decreto.

In caso di ricezione di una segnalazione tramite il Portale, il Responsabile della Gestione è tenuto a compiere i seguenti adempimenti:

- rilasciare al segnalante un avviso di ricevimento della segnalazione entro 7 giorni dalla data di ricezione: tecnicamente, al fine di garantire la massima tutela della riservatezza dell'identità del segnalante, il Portale non consente di inviare materialmente un vero e proprio avviso al predetto. Il segnalante potrà, tuttavia, prendere cognizione effettiva dell'avvenuta ricezione della propria segnalazione accedendo all'area a lui riservata tramite il "*key code*" ricevuto al momento dell'invio e visualizzando lo stato della segnalazione. Fino a quando il Responsabile della Gestione non avrà fatto accesso alla propria area riservata del Portale, lo stato della segnalazione verrà contrassegnato dalla dicitura "*nuova*". Al momento del primo accesso del Responsabile e di formale presa di cognizione del contenuto della segnalazione, il Portale trasformerà lo stato della segnalazione da "*nuova*" ad "*aperta*", in automatico e senza possibilità di ritorno allo stato iniziale da parte del Responsabile stesso (quest'ultimo, contestualmente all'avanzare dell'iter gestorio, potrà modificarne lo stato solo in senso progressivo e fino a quello definitivo di chiusura, di modo che il segnalante rimanga sempre aggiornato).
  La modifica dello stato della segnalazione da "*nuova*" ad "*aperta*", con l'indicazione del giorno e dell'ora dell'ultimo aggiornamento, operata in via automatica dal Portale, andrà considerata a tutti gli effetti alla stregua del cd. "avviso di ricevimento";
- in caso di segnalazione effettuata con comunicazione orale resa nell'ambito dell'incontro di persona richiesto dal segnalante, previa acquisizione del consenso espresso del segnalante, documentare la segnalazione mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale. In caso di redazione di verbale, il segnalante potrà verificarne, rettificarne e confermarne il contenuto mediante l'apposizione della propria sottoscrizione;
- mantenere le interlocuzioni con il segnalante, chiedendo – se del caso – chiarimenti e/o integrazioni, anche documentali, attraverso l'apposita area del Portale;
- dare un corretto ed effettivo seguito alle segnalazioni ricevute;

- fornire un riscontro al segnalante entro 3 mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro 3 mesi dalla scadenza del termine di 7 giorni dalla presentazione della segnalazione.

Per corretto ed effettivo seguito s'intende innanzitutto il rispetto di tempistiche ragionevoli e la necessità di garantire la riservatezza dei dati.

Il Responsabile della Gestione sarà chiamato inoltre a compiere un esame preliminare sulla sussistenza dei requisiti essenziali della segnalazione per valutarne l'ammissibilità e poter quindi accordare al segnalante le tutele previste, di cui si dirà meglio *infra*.

Per la valutazione dei suddetti requisiti, il Responsabile farà riferimento ai criteri indicati da ANAC nelle Linee Guida del 12.7.2023 e nelle eventuali successive integrazioni e/o modifiche.

In particolare, il Responsabile sarà tenuto a dichiarare:

- la manifesta infondatezza della segnalazione per l'eventuale assenza di elementi di fatto idonei a giustificare accertamenti;
- l'accertato contenuto generico della segnalazione qualora, dal suo contenuto, non sia possibile comprendere i fatti cui si riferisce ovvero in caso di segnalazione corredata da documentazione non appropriata o inconferente.

Una volta valutata l'ammissibilità della segnalazione ai fini dell'applicabilità del Decreto *Whistleblowing*, il Responsabile avvierà l'istruttoria interna sui fatti o sulle condotte segnalate per valutarne la sussistenza in concreto.

Per lo svolgimento dell'istruttoria, il Responsabile potrà avviare un dialogo con il segnalante, chiedendo allo stesso chiarimenti, documenti e informazioni ulteriori, sempre tramite il Portale o anche di persona. Ove necessario, il Responsabile potrà anche acquisire atti e documenti da altri uffici societari, avvalersi del loro supporto, coinvolgere terze persone, anche consulenti, tramite audizioni e altre richieste, avendo sempre cura che non sia compromessa la tutela della riservatezza del segnalante, del segnalato, delle altre persone eventualmente menzionate e del contenuto stesso della segnalazione. All'esito dell'istruttoria, il Responsabile fornirà un riscontro al segnalante.

Qualora, a seguito dell'attività svolta, vengano ravvisati elementi di manifesta infondatezza della segnalazione, ne sarà disposta l'archiviazione con adeguata motivazione.

Laddove, invece, si ravvisi il *fumus* di fondatezza della segnalazione, il Responsabile, in base all'oggetto e all'esito della segnalazione, dovrà rivolgersi immediatamente agli organi preposti interni alla Società, anche sul piano disciplinare, o agli enti/istituzioni esterne, ciascuno in funzione del proprio ambito di competenza.
Qualora, infine, dovesse emergere che la segnalazione è stata effettuata in malafede, il Responsabile della Gestione ne darà immediata comunicazione all'organo amministrativo della Società affinché attivi ogni iniziativa utile a perseguirne l'autore, sia sul piano disciplinare che davanti le competenti Autorità.

Non spetta, infatti, al Responsabile della Gestione accertare le responsabilità individuali qualunque natura esse abbiano, né svolgere controlli di legittimità o di merito su atti e provvedimenti adottati dall'ente/amministrazione oggetto di segnalazione.

Con riferimento al "*riscontro*" da effettuare entro il termine di 3 mesi, si evidenzia che lo stesso può consistere nella comunicazione dell'archiviazione, nell'avvio di un'inchiesta interna ed eventualmente nelle relative risultanze, nei provvedimenti adottati per affrontare la questione sollevata, nel rinvio a un'Autorità competente per lo svolgimento di ulteriori indagini.

Il medesimo riscontro può anche essere meramente interlocutorio, giacché possono essere comunicate le informazioni relative a tutte le attività sopra descritte che si intende intraprendere e lo stato di avanzamento dell'istruttoria. In tale ultimo caso, terminata l'istruttoria, gli esiti dovranno comunque essere comunicati al segnalante.

Qualora, per errore e/o colpa del segnalante, diversamente da quanto indicato nel presente Atto Organizzativo, la segnalazione di informazioni su violazioni rilevanti ai sensi del Decreto *Whistleblowing* dovesse avvenire internamente alla Società, ma attraverso un qualsiasi strumento diverso dal canale di segnalazione interna da questa attivato e con modalità differenti da quelle tecnicamente consentite dal Portale, il soggetto e/o la funzione aziendale che dovesse venire a conoscenza della segnalazione e del relativo contenuto, laddove il segnalante abbia dichiarato

espressamente di voler beneficiare delle tutele in materia *Whistleblowing* o tale volontà sia desumibile dalla segnalazione stessa, sarà tenuto ad osservare lo stesso obbligo di riservatezza che è posto a carico del Responsabile della Gestione e, attraverso il Portale *Whistleblowing*, entro il termine di 7 giorni dalla ricezione, dovrà trasmettere la segnalazione e ogni eventuale documento/file ad essa allegato al Responsabile della Gestione, attraverso l'avvio e la definizione della procedura ordinaria di invio di una nuova segnalazione, dandone contestuale comunicazione – laddove materialmente possibile – al segnalante. In caso contrario la segnalazione verrà gestita in via ordinaria e, dunque, senza l'applicazione delle tutele e delle garanzie previste dal Decreto.

2.3 Canali di segnalazione esterna

Per segnalazione esterna s'intende "*la comunicazione, scritto od orale, delle informazioni sulle violazioni, presentata tramite il canale di segnalazione esterna di cui all'art. 7*".

Le segnalazioni esterne possono essere inviate solo dai soggetti di cui all'art. 3 del Decreto *Whistleblowing* (premesso che per segnalante, come già indicato, s'intende la persona fisica[2] che effettua la segnalazione, si tratta dei soggetti già indicati nel pr. *sub* 1.3 "*Destinatari*" con riferimento alle segnalazioni interne).

Ferma restando la preferenza per i canali di segnalazione interna, il D.Lgs. n. 24/2023, al ricorrere delle condizioni espressamente disciplinate dall'art. 6, prevede la possibilità di effettuare una segnalazione attraverso i canali di segnalazione esterna.

In particolare, il segnalante può effettuare una segnalazione esterna se, al momento della sua presentazione:

- il canale interno, pur essendo obbligatorio, non è attivo o, anche se regolarmente attivato, non è conforme a quanto previsto dal Decreto con riferimento alle modalità di presentazione delle segnalazioni interne, ai soggetti che possono gestirne la relativa trattazione e, in generale, con riferimento al sistema di tutele e garanzie che devono essere assicurate in concreto;

[2] Non sono prese in considerazione, pertanto, le segnalazioni presentate da altri soggetti, ivi inclusi i rappresentanti di organizzazioni sindacali, in quanto l'istituto del *Whistleblowing* è indirizzato alla tutela della singola persona fisica che agisce in suo nome e per suo conto, non spendendo la sigla sindacale.

- il segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito da parte della persona o dell'ufficio designati (si fa riferimento ai casi in cui il canale interno sia stato utilizzato ma non abbia funzionato correttamente, nel senso che la segnalazione non è stata trattata entro un termine ragionevole, oppure non è stata intrapresa un'azione per affrontare la violazione);
- il segnalante ha fondati motivi di ritenere ragionevolmente, sulla base di circostanze concrete allegate ed informazioni effettivamente acquisibili, e, quindi, non su semplici illazioni, che, se effettuasse una segnalazione interna
- alla stessa non sarebbe dato efficace seguito (ciò si verifica quando, ad esempio, il responsabile ultimo nel contesto lavorativo sia coinvolto nella violazione, vi sia il rischio che la violazione o le relative prove possano essere occultate o distrutte, l'efficacia delle indagini svolte dalle Autorità competenti potrebbe essere altrimenti compromessa o anche perché si ritiene che ANAC sarebbe più indicata ad affrontare la specifica violazione, soprattutto nelle materie di propria competenza);
- questa potrebbe determinare il rischio di ritorsione (anche come conseguenza della violazione dell'obbligo di riservatezza dell'identità del segnalante);
- il segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse (ad esempio, il caso in cui la violazione richieda un intervento urgente, per salvaguardare la salute e la sicurezza delle persone o per proteggere l'ambiente).

La gestione dei canali di segnalazione esterna è affidata esclusivamente ad ANAC.

ANAC al momento ha provveduto all'attivazione dei seguenti canali di segnalazione esterna:

- piattaforma informatica (comunicazione scritta);
- servizio telefonico con operatore (comunicazione orale);
- richiesta di fissazione di un incontro diretto per comunicare oralmente la segnalazione esterna.

Per l'esame completo delle modalità di invio e gestione delle segnalazioni esterne, si rinvia alla specifica sezione contenuta nelle Linee Guida ANAC del 12.7.2023 e alle eventuali successive modifiche/integrazioni.

Da ultimo, come verrà indicato più specificatamente nel paragrafo riguardante le tutele, secondo quanto previsto dall'art. 19 del D.Lgs. n. 24/2023, il segnalante e gli altri soggetti di cui all'art. 3, comma 5, possono comunicare ad ANAC, tramite piattaforma informatica, le ritorsioni che ritengono di avere subito in ragione della segnalazione, della denuncia all'Autorità giudiziaria o contabile o della divulgazione pubblica.

2.4 Divulgazione pubblica

Il Decreto *Whistleblowing* ha previsto un'ulteriore modalità di segnalazione consistente nella divulgazione pubblica.

Per "divulgazione pubblica" s'intende "*rendere di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone*".

Nel concetto di mezzi di diffusione sono inclusi anche i *social network*, così come le comunicazioni ai rappresentanti eletti, alle organizzazioni della società civile, ai sindacati o alle organizzazioni imprenditoriali e professionali.

Ai sensi dell'art. 15, l'autore della divulgazione pubblica beneficia della protezione prevista dal Decreto *Whistleblowing* soltanto laddove, al momento della divulgazione pubblica, ricorra almeno una delle seguenti condizioni:

a) il segnalante ha previamente effettuato una segnalazione interna ed esterna ovvero ha effettuato direttamente una segnalazione esterna e ad essa non è stato dato riscontro nei termini previsti (per la segnalazione interna, 3 mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro 3 mesi dalla scadenza del termine di 7 giorni dalla presentazione della segnalazione; per la segnalazione esterna, 3 mesi o, se ricorrono giustificate e motivate ragioni, 6 mesi dalla data di avviso di ricevimento della segnalazione esterna o, in mancanza di detto avviso, dalla scadenza dei 7 giorni dal ricevimento);

b) il segnalante ha fondato motivo di ritenere, ragionevolmente, sulla base di circostanze concrete, che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse (i.e. una situazione di emergenza o il rischio di danno irreversibile, anche all'incolumità fisica di una o più

persone), che richiedono che la violazione sia svelata prontamente e abbia un'ampia risonanza per impedirne gli effetti;
c) il segnalante ha fondato motivo di ritenere, ragionevolmente, sulla base di circostanze concrete, che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto (ad esempio, perché teme che possano essere occultate o distrutte prove oppure che chi ha ricevuto la segnalazione possa essere colluso con l'autore della violazione o coinvolto nella violazione stessa).

Il soggetto che effettua una divulgazione pubblica deve considerarsi distinto da chi costituisce fonte di informazione per i giornalisti[3].

Laddove il soggetto riveli volontariamente la propria identità, non opereranno le disposizioni in tema di tutela della riservatezza, ferme restando tutte le altre forme di protezione previste dal Decreto.

Nell'ipotesi in cui, invece, la divulgazione avvenga mediante l'utilizzo di uno pseudonimo o di un *nickname*, che non consenta l'identificazione dell'autore, ANAC tratterà la divulgazione alla stregua di una segnalazione anonima e avrà cura di registrarla, ai fini della conservazione, per garantire al divulgatore, in caso di disvelamento successivo dell'identità dello stesso, le tutele previste nel caso in cui lo stesso comunichi di subire ritorsioni.

2.5 Denuncia all'Autorità giudiziaria e/o contabile

Il Decreto *Whistleblowing* riconosce ai soggetti tutelati anche la possibilità di rivolgersi alle Autorità giudiziarie, per inoltrare una denuncia di condotte illecite di cui siano venuti a conoscenza in un contesto lavorativo pubblico o privato.
Si precisa che, qualora il segnalante rivesta la qualifica di pubblico ufficiale o di incaricato di pubblico servizio, anche laddove lo stesso abbia effettuato una segnalazione attraverso i canali interni o esterni previsti dal Decreto, ciò non lo esonera dall'obbligo di denunciare alla competente Autorità giudiziaria i fatti penalmente rilevanti e le ipotesi di danno erariale.

[3] Il Decreto prevede che restino ferme le norme sul segreto professionale degli esercenti la professione giornalistica, con riferimento alla fonte della notizia. In tal caso, il soggetto che fornisce informazioni costituisce una fonte per il giornalismo di inchiesta ed esula dalle finalità perseguite con il D.Lgs. n. 24/2023.

3. SISTEMA DI PROTEZIONE PREVISTO DAL DECRETO WHISTLEBLOWING

3.1 Soggetti che godono delle misure di protezione

Uno dei principali aspetti dell'intera disciplina di cui al Decreto Whistleblowing è rappresentato dal sistema di tutele previste in favore di colui che segnala, effettua una divulgazione pubblica o denuncia violazioni[4].

Tali tutele verranno approfondite nei successivi paragrafi della presente sezione dell'Atto Organizzativo.

Tuttavia, deve essere sin d'ora specificato che il sistema di protezione approntato dal Legislatore si estende anche a soggetti diversi dal segnalante, denunciante o dall'autore della divulgazione pubblica, ricomprendendo anche quei soggetti che, in ragione del ruolo assunto nell'ambito del processo di segnalazione, denuncia o divulgazione pubblica e/o del particolare rapporto che li lega al segnalante o denunciante, potrebbero essere destinatari di ritorsioni, intraprese anche indirettamente.

Ai sensi dell'art. 3, comma 5, le misure di protezione di cui al capo III del Decreto sono riconosciute anche ai seguenti soggetti (per ulteriori approfondimenti sull'individuazione in concreto di tali soggetti, si rimanda alle Linee Guida ANAC del 12.7.2023 e alle eventuali successive modifiche/integrazioni):
ai facilitatori[5];

- alle persone del medesimo contesto lavorativo del segnalante, di colui che ha sporto una denuncia all'autorità giudiziaria o contabile o di colui che ha effettuato una divulgazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;
- ai colleghi di lavoro del segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o effettuato una divulgazione pubblica, che lavorano nel medesimo

[4] Tali soggetti sono stati in precedenza indicati nel pr. *sub* 1.3 "*Destinatari*".
[5] Persona fisica che assiste il segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata.

contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;

- agli enti di proprietà del segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o che ha effettuato una divulgazione pubblica o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone.

3.2 Tutela della riservatezza

Il sistema di protezione previsto dal Decreto e adottato dalla Società attraverso l'esecuzione di tutti gli adempimenti ivi disciplinati garantisce la riservatezza dell'identità del segnalante (inclusa ogni informazione, anche desumibile dalla documentazione eventualmente allegata, da cui essa possa desumersi direttamente o indirettamente), del facilitatore, della persona coinvolta e delle altre persone eventualmente menzionate nella segnalazione (anche quando quest'ultima avviene in forme diverse da quelle prescritte o perviene a soggetti diversi dal Responsabile della Gestione).

L'art. 12 del Decreto sancisce, infatti, l'obbligo di riservatezza, stabilendo che:

- comma 1 – le segnalazioni non possono essere utilizzate oltre quanto necessario per dare alle stesse adeguato seguito (principio di limitazione delle finalità e minimizzazione dei dati - inoltre, ai sensi dell'art. 13, c. 2, "*I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente*");
- comma 2 – l'identità del segnalante e qualsiasi altra informazione da cui essa può evincersi, direttamente o indirettamente, non possono essere rivelate senza il consenso espresso del predetto a persone diverse dal Responsabile della Gestione;
- comma 3 – nell'ambito del procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'art. 329 c.p.p.[6];
- comma 4 – nell'ambito del procedimento dinnanzi alla Corte dei Conti, l'identità del segnalante non può essere rivelata fino alla chiusura della fase istruttoria (successivamente, potrà essere disvelata dall'Autorità contabile al fine di essere utilizzata nel procedimento stesso);

[6] Tale disposizione prevede l'obbligo del segreto sugli atti compiuti nelle indagini preliminari "*fino a quando l'imputato non ne possa avere conoscenza e, comunque, non oltre la chiusura delle indagini preliminari*".

- comma 5 – nell'ambito del procedimento disciplinare, l'identità del segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile solo in presenza del consenso espresso del segnalante alla rivelazione della propria identità;
- comma 6 – è dato avviso al segnalante mediante comunicazione scritta delle ragioni della rivelazione dei dati riservati, nell'ipotesi di cui al comma 5 (proc. disciplinare), secondo periodo, nonché nelle procedure di segnalazione interna ed esterna di cui al presente capo quando la rivelazione dell'identità del segnalante e delle informazioni di cui al comma 2 è indispensabile anche ai fini della difesa della persona coinvolta;
- comma 7 – i soggetti del settore pubblico e del settore privato, ANAC, nonché le Autorità amministrative cui ANAC trasmette le segnalazioni esterne di loro competenza, tutelano l'identità delle persone coinvolte e delle persone menzionate nella segnalazione fino alla conclusione dei procedimenti avviati nel rispetto delle medesime garanzie previste in favore del segnalante;
- comma 8 – la segnalazione è sottratta all'accesso previsto dagli artt. 22 e ss. della L. n. 241/1990, nonché dagli artt. 5 e ss. del d.lgs. n. 33/2013;
- comma 9 – ferma la previsione dei commi da 1 a 8, nelle procedure di segnalazione interna ed esterna, la persona coinvolta può essere sentita, ovvero, su sua richiesta, è sentita, anche mediante procedimento cartolare attraverso l'acquisizione di osservazioni scritte e documenti.

La tutela della riservatezza delle persone coinvolte o menzionate nella segnalazione non si estende al caso di denuncia all'Autorità Giudiziaria e alla Corte dei Conti. In queste ultime due ipotesi il Legislatore circoscrive la tutela al solo segnalante. Per quanto riguarda, inoltre, l'ipotesi di divulgazione pubblica, la protezione della riservatezza non si applica nel caso in cui il segnalante abbia intenzionalmente rivelato la propria identità mediante, ad esempio, piattaforme *web* o *social media*. Lo stesso vale nell'ipotesi in cui il soggetto si rivolga direttamente ad un giornalista.

Nel caso in cui, invece, colui che effettua la divulgazione non riveli la propria identità (ad es. utilizzando uno pseudonimo o un *nickname* nel caso di *social*), tali divulgazioni sono equiparabili alle segnalazioni anonime.

Con l'adozione del MOGC 231, la Società provvederà a definire un sistema sanzionatorio *ad hoc* che preveda l'irrogazione di sanzioni disciplinari nei confronti di coloro che verranno ritenuti responsabili della violazione dell'obbligo di riservatezza di cui all'art. 12 del Decreto *Whistleblowing*.

3.3 Diritto alla protezione dei dati personali

Al fine di garantire il diritto alla protezione dei dati personali al segnalante o denunciante il Legislatore ha previsto che l'acquisizione e gestione delle segnalazioni, divulgazioni pubbliche o denunce, ivi incluse le comunicazioni tra le Autorità competenti, avvenga in conformità alla normativa in tema di tutela dei dati personali [in particolare il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio (GDPR) e al D.Lgs. n. 196/2003].

Qualsiasi scambio e trasmissione di informazioni che comporti un trattamento di dati personali da parte delle istituzioni, organi o organismi dell'UE deve inoltre avvenire in conformità al regolamento (UE) 2018/1725.

La tutela dei dati personali è assicurata non solo alla persona segnalante o denunciante ma anche agli altri soggetti cui si applica la tutela della riservatezza, quali il facilitatore, la persona coinvolta e la persona menzionata nella segnalazione, in quanto "interessati" dal trattamento dei dati.
Di seguito vengono indicate le qualifiche dei soggetti che possono trattare i dati personali legati alla presente disciplina:

- Titolare del trattamento:
  - per il canale di segnalazione interna: la Società;
  - per il canale di segnalazione esterna: ANAC e/o le altre Autorità a cui vengono trasmesse le segnalazioni;
- Contitolari del trattamento:
  - enti pubblici e/o privati nell'ipotesi in cui condividano il medesimo canale di segnalazione interna;
- Responsabile del trattamento:
  - fornitore del Portale *Whistleblowing*;
  - Responsabile della Gestione del canale di segnalazione interna (se si tratta un soggetto esterno alla Società);

- Soggetto autorizzato al trattamento:
  - Responsabile della Gestione del canale di segnalazione interna (se si tratta di un soggetto interno alla Società, incluso eventualmente l'Organismo di Vigilanza previsto *ex* D.Lgs. n. 231/2001) e le persone espressamente designate dal Titolare o dai Contitolari del trattamento che trattano le segnalazioni.

La documentazione concernente le segnalazioni e i dati ad essa relativi sono riservati. Tale documentazione deve essere archiviata in maniera sicura e nel rispetto delle procedure aziendali sulla classificazione e trattamento delle informazioni e per il tempo necessario alla gestione della segnalazione e, comunque, non oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

In caso di violazione della normativa sopra richiamata, l'interessato potrà rivolgersi al Garante per la protezione dei dati personali.

3.4 Tutela da eventuali misure ritorsive

Il Decreto *Whistleblowing* vieta di adottare qualsiasi misura ritorsiva nei confronti del segnalante e degli altri soggetti espressamente tutelati.

Per ritorsione s'intende "*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* (ndr. anche l'ente)*, in via diretta o indiretta, un danno ingiusto*".

Si tratta, quindi, di una definizione ampia del concetto di ritorsione che può consistere sia in atti o provvedimenti ma anche in comportamenti od omissioni che si verificano nel contesto lavorativo e che arrecano pregiudizio ai soggetti tutelati, includendo anche quelle solo tentate o minacciate.

Per "*ritorsione tentata*" s'intende, ad esempio, il licenziamento come conseguenza di una segnalazione, denuncia o divulgazione pubblica che il datore di lavoro non è riuscito a realizzare per un mero vizio formale commesso nella procedura di licenziamento; per "*ritorsione minacciata*" s'intende, ad esempio, la prospettazione del licenziamento o del mutamento delle funzioni avvenuta

nel corso di un colloquio che chi ha segnalato, denunciato o effettuato una divulgazione ha avuto con il proprio datore di lavoro (in entrambi i casi il soggetto tutelato deve necessariamente fornire elementi da cui poter desumere il *fumus* sull'effettività del tentativo ritorsivo o della minaccia).

L'art. 17, comma 4, prevede un elenco (dal carattere non esaustivo e/o tassativo) delle possibili misure ritorsive:

- licenziamento, sospensione o misure equivalenti;
- retrocessione di grado o mancata promozione;
- mutamento di funzioni, cambiamento del luogo di lavoro, riduzione dello stipendio, modifica dell'orario di lavoro;
- sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
- note di demerito o referenze negative;
- adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
- coercizione, intimidazione, molestie o ostracismo;
- discriminazione o comunque trattamento sfavorevole;
- mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
- mancato rinnovo o risoluzione anticipata di un contratto di lavoro a termine;
- danni, anche alla reputazione della persona, in particolare sui social media, o pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;
- inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro;
- conclusione anticipata o annullamento del contratto di fornitura di beni o servizi;
- annullamento di una licenza o di un permesso;
- richiesta di sottoposizione ad accertamenti psichiatrici o medici.

Secondo quanto previsto dall'art. 19 del D.Lgs. n. 24/2023, l'adozione di eventuali misure ritorsive può essere comunicata ad ANAC dal segnalante e dagli altri soggetti di cui all'art. 3, comma 5, tramite la piattaforma informatica da quest'ultima predisposta.
L'art. 16 stabilisce le condizioni la cui sussistenza è necessaria per poter beneficiare della protezione prevista dal Decreto *Whistleblowing*:

- comma 1, lett. a): "*al momento della segnalazione o della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica, la persona segnalante o denunciante aveva fondato motivo di ritenere che le informazioni sulle violazioni segnalate, divulgate pubblicamente o denunciate fossero vere e rientrassero nell'ambito oggettivo di cui all'articolo 1*". È, dunque, necessario che il segnalante, colui che ha denunciato o ha effettuato la divulgazione pubblica abbiano agito in tal senso in base ad una convinzione ragionevole che le informazioni sulle violazioni segnalate, divulgate o denunciate fossero veritiere e rientranti nell'ambito oggettivo di applicazione del Decreto (non sono sufficienti invece i meri sospetti o le voci di corridoio – cd. requisito della pertinenza). Non rileva invece, ai fini del riconoscimento delle tutele, la circostanza che il soggetto abbia segnalato, effettuato divulgazioni pubbliche o denunce pur non essendo certo dell'effettivo accadimento dei fatti segnalati o denunciati e/o dell'identità dell'autore degli stessi o riportando anche fatti inesatti per via di un errore genuino;
- comma 1, lett. b): "*la segnalazione o divulgazione pubblica è stata effettuata sulla base di quanto previsto dal capo II*".

  Le condizioni di cui ai due punti che precedono devono sussistere congiuntamente e deve esserci uno stretto collegamento tra segnalazione/denuncia/divulgazione pubblica e il comportamento/atto/omissione sfavorevole subito, direttamente o indirettamente, affinché questi ultimi possano essere considerati come "ritorsione" e il soggetto che li ha subiti possa beneficiare della protezione prevista dal Decreto (nesso di causalità che dovrà essere accertato da ANAC).

  La medesima forma di tutela si applica anche al cd. "facilitatore" e agli altri soggetti assimilati al segnalante (già indicati per esteso nel pr. *sub* 3.1 "*Soggetti che godono delle misure di protezione indicate nella presente sezione dell'Atto Organizzativo*"), i quali – al ricorrere delle medesime condizioni – possono comunicare ad ANAC le eventuali misure ritorsive, adottate nei loro confronti in ragione del legame qualificato con il segnalante, denunciante o divulgatore pubblico.

Se difettano le condizioni previste dall'art. 16:

a. le segnalazioni, divulgazioni pubbliche e denunce non saranno considerate come rientranti nell'ambito della disciplina *Whistleblowing* e quindi le tutele previste non verranno riconosciute in favore del segnalante, dell'autore della denuncia o di chi ha effettuato la divulgazione pubblica;

b. analogamente si esclude la protezione riconosciuta ai soggetti diversi, che in ragione del ruolo assunto nell'ambito del processo di segnalazione/denuncia e/o del particolare rapporto che li lega al segnalante o denunciante, siano stati destinatari di uno degli atti, comportamenti o provvedimenti sopra indicati.

L'art. 16, comma 3, stabilisce inoltre che "*Salvo quanto previsto dall'art. 20, quando è accertata, anche con sentenza di primo grado, la responsabilità penale della persona segnalante per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave, le tutele di cui al presente capo non sono garantite e alla persona segnalante o denunciante è irrogata una sanzione disciplinare*"[7].

L'art. 16, comma 4, da ultimo, stabilisce che "*La disposizione di cui al presente articolo si applica anche nei casi di segnalazione o denuncia all'autorità giudiziaria o contabile o divulgazione pubblica anonime, se la persona segnalante è stata successivamente identificata e ha subito ritorsioni, nonché nei casi di segnalazione presentata alle istituzioni, agli organi e agli organismi competenti dell'Unione europea, in conformità alle condizioni di cui all'articolo 6*".

3.5 Misure di sostegno da parte di enti del Terzo settore

Ad ulteriore rafforzamento della protezione del segnalante, ai sensi dell'art. 18 del Decreto, è prevista la possibilità che ANAC stipuli convenzioni con enti del Terzo settore affinché questi ultimi forniscano misure di sostegno al segnalante.

In particolare, tali enti, inseriti in un apposito elenco pubblicato da ANAC sul proprio sito istituzionale, prestano assistenza e consulenza a titolo gratuito sulle modalità di segnalazione, sulla protezione dalle ritorsioni riconosciuta dalle disposizioni normative nazionali e da quelle dell'Unione europea, sui diritti della persona coinvolta, sulle modalità e condizioni di accesso al patrocinio a spese dello Stato.

[7] ANAC ha evidenziato, tuttavia, che le tutele previste dal Decreto possano essere applicate anche successivamente, qualora la sentenza di condanna dovesse essere poi riformata in senso favorevole al segnalante o autore della denuncia.

3.6 Limitazioni di responsabilità per chi segnala, denuncia o effettua divulgazioni pubbliche

Tra le tutele riconosciute al segnalante, denunciante o a chi effettua una divulgazione pubblica si devono annoverare anche le limitazioni della responsabilità rispetto alla rivelazione e alla diffusione di alcune categorie di informazioni.

Si tratta di limitazioni che operano al ricorrere di determinate condizioni in assenza delle quali vi sarebbero conseguenze in termini di responsabilità penale, civile, amministrativa.

Qualora operi la scriminante, nei casi di diffusione di informazioni coperte dall'obbligo di segreto, non saranno configurabili i seguenti reati:

- rivelazione e utilizzazione del segreto d'ufficio (art. 326 c.p.);
- rivelazione del segreto professionale (art. 622 c.p.);
- rivelazione dei segreti scientifici e industriali (art. 623 c.p.);
- violazione del dovere di fedeltà e di lealtà (art. 2105 c.c.).

Né saranno configurabili responsabilità per:

- violazione delle disposizioni relative al diritto d'autore;
- violazione delle disposizioni relative alla protezione dei dati personali;
- rivelazione o diffusione di informazioni sulle violazioni che offendono la reputazione della persona coinvolta.

Le limitazioni di responsabilità operano solo nei casi in cui ricorrano due condizioni:

1. al momento della rivelazione o diffusione vi siano fondati motivi per ritenere che le informazioni siano necessarie per far scoprire la violazione. La persona, quindi, deve ragionevolmente ritenere, e non in base a semplici illazioni, che quelle informazioni debbano svelarsi perché indispensabili per far emergere la violazione, ad esclusione di quelle superflue, e non per ulteriori e diverse ragioni (ad esempio, *gossip*, fini vendicativi, opportunistici o scandalistici);
2. la segnalazione, la divulgazione pubblica o la denuncia sia stata effettuata nel rispetto delle condizioni previste dal Decreto per beneficiare della tutela dalle ritorsioni.

Qualora entrambe le condizioni risultino soddisfatte, le persone che segnalano, denunciano o effettuano una divulgazione pubblica non incorreranno in alcun tipo di responsabilità civile, penale, amministrativa o disciplinare.

L'ente o la persona tutelata ai sensi del Decreto andrà esente da responsabilità, anche di natura civile o amministrativa, per l'acquisizione delle informazioni sulle violazioni o per l'accesso alle stesse, purché tale acquisizione/accesso sia avvenuto in modo lecito e non costituisca "di per sé" un reato.
Ove l'acquisizione o l'accesso alle informazioni o ai documenti sia stato ottenuto commettendo un reato, come un accesso abusivo o un atto di pirateria informatica, l'esclusione della responsabilità non opera ma resta ferma la responsabilità penale, e ogni altra responsabilità anche civile, amministrativa e disciplinare e spetterà all'Autorità giudiziaria valutare la responsabilità della persona o dell'ente segnalante, denunciante, che ha effettuato la divulgazione pubblica alla luce di tutte le informazioni fattuali pertinenti e tenendo conto delle circostanze specifiche del caso.

La scriminante opera con riguardo ai comportamenti, agli atti o alle omissioni poste in essere solo se collegati alla segnalazione, denuncia o divulgazione pubblica e se sono strettamente necessari a rivelare la violazione.

Affinché le responsabilità non vengano in rilievo, quindi, deve, innanzitutto, aversi una stretta connessione tra la segnalazione, denuncia o divulgazione pubblica con quanto compiuto o omesso.

Inoltre, il compimento degli atti, comportamenti, omissioni deve essere strettamente necessario, e quindi non superfluo, perché la violazione possa emergere.

In assenza di queste condizioni la responsabilità deve ritenersi non esclusa e potrà essere valutata dall'Autorità giudiziaria, caso per caso, considerando tutte le informazioni fattuali disponibili e tenendo conto delle circostanze specifiche del caso, comprese la necessità e la proporzionalità dell'atto o dell'omissione in relazione alla segnalazione, denuncia, o alla divulgazione.

3.7 Divieto di rinunce e transazioni

Non sono valide le rinunce e le transazioni, integrali o parziali, che abbiano per oggetto i diritti e le tutele previsti dal Decreto *Whistleblowing*, salvo che esse siano effettuate nelle cd. sedi protette di cui

all' art. 2113, c. 4, c.c. [i.e., accordi conclusi in sede giudiziale (art. 185 c.p.c.)]; dinanzi alla commissione di conciliazione istituita presso la Direzione territoriale del lavoro (art. 410 c.p.c.); innanzi alle sedi di certificazione (art. 31, c. 13, L. n. 183/2010); innanzi alla Commissione di conciliazione istituita in sede sindacale (art. 412-ter c.p.c.); presso i Collegi di conciliazione ed arbitrato irrituale (art. 412-quater c.p.c.).

A maggior ragione, tali tutele non possono essere oggetto di rinuncia volontaria.

Lombardi Ingegneria S.r.l. – Socio Unico
Via Giotto 36, IT-20145 Milano
Telefono +39 02 583 03 324, Fax +39 02 583 03 190
milano@lombardi.group, www.lombardi.group

Unità locale Roma
Via XX Settembre 98/G, IT-00185 Roma, Italy

Unità locale Torino
Via R. Montecuccoli 9, IT-10121 Torino, Italy
torino@lombardi.group, www.lombardi.group

Certificato SGS ISO 9001:2015 | CH97/0470
Certificato SGS ISO 14001:2015 | CH16/0455
Certificato SGS ISO 45001:2018 | CH21/0629
C.F./P.I.: N°12151290157, Reg. Imprese di Milano N° 12151290157
R.E.A. di Milano N° 1530711, Capitale sociale € 110.000,00

4. FORMAZIONE E INFORMAZIONE SUI CONTENUTI DEL DECRETO WHISTLEBLOWING

La Società considera la formazione e l'informazione sui contenuti del Decreto *Whistleblowing* quale elemento fondamentale per assolvere correttamente alle finalità postulate dalla predetta normativa.

Per tali ragioni, la Società si impegna ad assicurare un costante aggiornamento della formazione dei propri dipendenti in materia di *Whistleblowing*, al fine di evidenziare i comportamenti meritevoli di segnalazione ed evitare che si verifichino condotte inappropriate o illegittime.

Allo stesso modo la Società si impegna a promuovere la conoscenza e l'aggiornamento della disciplina *Whistleblowing* nei rapporti con le terze parti (clienti, fornitori, consulenti, collaboratori e terzisti), assicurando adeguata pubblicità ai contenuti del presente Atto Organizzativo e, ove richiesto e/o opportuno, adottando apposite clausole nei contratti che regolano diritti e obblighi di ciascuna parte contraente.

Lombardi Ingegneria S.r.l. – Socio Unico
Via Giotto 36, IT-20145 Milano
Telefono +39 02 583 03 324, Fax +39 02 583 03 190
milano@lombardi.group, www.lombardi.group

Unità locale Roma
Via XX Settembre 98/G, IT-00185 Roma, Italy

Unità locale Torino
Via R. Montecuccoli 9, IT-10121 Torino, Italy
torino@lombardi.group, www.lombardi.group

Certificato SGS ISO 9001:2015 | CH97/0470
Certificato SGS ISO 14001:2015 | CH16/0455
Certificato SGS ISO 45001:2018 | CH21/0629
C.F./P.I.: N°12151290157, Reg. Imprese di Milano N° 12151290157
R.E.A. di Milano N° 1530711, Capitale sociale € 110.000,00

5. AGGIORNAMENTO DEL PRESENTE ATTO ORGANIZZATIVO

Il presente Atto Organizzativo, il Portale *Whistleblowing* e la documentazione afferente ognuna delle prescrizioni attualmente previste dal D.Lgs. n. 24/2023 saranno oggetto di revisione e aggiornamento periodico al fine di garantire il loro costante allineamento alla normativa di riferimento.

Lombardi Ingegneria S.r.l. – Socio Unico
Via Giotto 36, IT-20145 Milano
Telefono +39 02 583 03 324, Fax +39 02 583 03 190
milano@lombardi.group, www.lombardi.group

Unità locale Roma
Via XX Settembre 98/G, IT-00185 Roma, Italy

Unità locale Torino
Via R. Montecuccoli 9, IT-10121 Torino, Italy
torino@lombardi.group, www.lombardi.group

Certificato SGS ISO 9001:2015 | CH97/0470
Certificato SGS ISO 14001:2015 | CH16/0455
Certificato SGS ISO 45001:2018 | CH21/0629
C.F./P.I.: N°12151290157, Reg. Imprese di Milano N° 12151290157
R.E.A. di Milano N° 1530711, Capitale sociale € 110.000,00

6. ALLEGATI

Al presente Atto Organizzativo vengono allegati i seguenti documenti:

- all. 1a: dichiarazione di conformità del Portale *Whistleblowing*, rilasciata da ISWEB S.p.A.;
- all. 1b: dichiarazione sulle misure di sicurezza del Portale *Whistleblowing*, rilasciata da ISWEB S.p.A.;
- all. 1c: certificato "ISWEB Cloud", rilasciato da ISWEB S.p.A.;
- all. 2: form del modulo di segnalazione presente sul Portale *Whistleblowing*, fornito da ISWEB S.p.A..

Lombardi Ingegneria S.r.l. – Socio Unico
Via Giotto 36, IT-20145 Milano
Telefono +39 02 583 03 324, Fax +39 02 583 03 190
milano@lombardi.group, www.lombardi.group

Unità locale Roma
Via XX Settembre 98/G, IT-00185 Roma, Italy

Unità locale Torino
Via R. Montecuccoli 9, IT-10121 Torino, Italy
torino@lombardi.group, www.lombardi.group

Certificato SGS ISO 9001:2015 | CH97/0470
Certificato SGS ISO 14001:2015 | CH16/0455
Certificato SGS ISO 45001:2018 | CH21/0629
C.F./P.I.: N°12151290157, Reg. Imprese di Milano N° 12151290157
R.E.A. di Milano N° 1530711, Capitale sociale € 110.000,00

CERTIFICAZIONE DI COMPLIANCE WHISTLEBLOWING/PAWHISTLEBLOWING

Classificazione documento:	Controllato
Data Ultimo aggiornamento:	29/09/2023

www.isweb.it

ISWEB S.p.A.
Via Cadorna 31 - 67051 Avezzano (AQ)
Via Fiume Giallo 3 - 00144 Roma

ISO 9001-2015 - RINA
Sistema di gestione della qualità certificato RINA
Certificato n° 14770/06/S

Numero Verde Gratuito
800 97 34 34

Indice

1. Introduzione

Il presente documento è una autocertificazione delle misure di sicurezza applicate nello sviluppo del servizio **Whistleblowing** basato sul software Open Source Globaleaks e manutenuto da ISWEB S.p.a. ed ha lo scopo di certificarne il livello di adeguamento rispetto alle nuove misure di protezione introdotte dal regolamento UE 2016/679, in merito alla privacy dei cittadini della comunità europea.

1.1 Contesto applicativo

Il servizio Whistleblowing consiste in una piattaforma informatica per la raccolta di segnalazioni di comportamenti illeciti o di violazioni ai modelli organizzativi adottati dall'ente o azienda cliente.
La piattaforma informatica utilizzata per il servizio è un software interamente web-based che non necessità l'installazione di alcun componente sul client dell'utilizzatore, ed ha un'architettura three-tier:

- Interfaccia -> webapp realizzata in angular JS
- Business Logic -> componente backed server realizzata python
- Dati -> database per i dati realizzato su SQL Lite

1.2 Dati trattati e modalità di acquisizione

L'applicazione si compone di un unico modulo per la raccolta dei seguenti tipi di dati, in funzione delle esigenze del Committente:

- Informazioni anagrafiche basilari dell'utilizzatore (facoltativi di default): il form raccoglie i dati anagrafici del segnalante, secondo le esigenze del Committente, come nome, cognome, data di nascita, codice fiscale e dati di recapito (indirizzo, email, telefono)
- Informazioni sulla segnalazione: il form raccoglie le informazioni relative alla segnalazione, come ad esempio le tempistiche in cui essa è avvenuta, il tipo di condotta scorretta, ed i dati nominativi degli eventuali soggetti fisici o giuridici coinvolti. Anche in questo caso la struttura del form di segnalazione può essere definita dal Committente

Si precisa che il form dispone di diversi campi a compilazione libera.

Si precisa che tutti i dati sono inviati, trattati e archiviati su server siti all'interno dell'UE, sulla infrastruttura server dedicata ISWEB ospitata dai nostri partner. Per maggiori dettagli sull'infrastruttura, si invita a consultare la documentazione allegata all'offerta commerciale.

[Art. 4 GDPR]
La struttura dei dati raccolti può variare in funzione delle esigenze del committente. Anche l'utilizzo obbligatorio o facoltativo del form di iscrizione è un aspetto che può variare in funzione delle esigenze del committente.

[Art. 9 GDPR]
Il servizio non prevede la richiesta o il trattamento di dati appartenenti a categorie particolari, come opinioni sessuali, politiche o religiose.

1.3 Dati di navigazione e COOKIE

Visto il particolare contesto applicativo, il log tecnico di servizio applicativo per Whistleblowing non memorizza alcun dato personale **rimuovendo l'indirizzo IP e le caratteristiche dell'user agent utilizzato per le richieste in fase di mappatura**.
I dati mantenuti sono quindi relativi alle sole informazioni tecniche di servizio:

- Orario, tipo e protocollo di richiesta
- Risorsa richiesta
- Tempo e codice della risposta

La piattaforma inoltre fa utilizzo esclusivamente di cookie tecnici per il suo utilizzo, e non utilizza alcun tipo di cookie di profilazione e/o di terze parti.
Anche livello infrastrutturale di routing dei pacchetti inoltre, la crittografia del protocollo di comunicazione implica l'impossibilità attraverso il contenuto dei dati in transito di associare l'indirizzo IP dei navigatori con specifici dati personali al di fuori dei provider delle specifiche connettività di questi ultimi.

1.4 Data Retention

Il periodo di mantenimento è definito dal Committente tramite le funzionalità della piattaforma, e comunque con un massimale configurabile in fase di attivazione del servizio.

2. Misure di sicurezza e correttivi per garantire i livelli di sicurezza richiesti

Per il servizio Whistleblowing sono stati implementate le seguenti misure di sicurezza al fine di garantire un livello di protezione adeguato al tipo di dati personali che raccoglie, come dichiarati in Sezione 1.

MISURA DI SICUREZZA	APPLICATA
Il team di sviluppo ha seguito le linee guida della OWASP per lo sviluppo di applicazioni Web sicure.	Si, il software Globaleaks è stato sviluppato seguendo le linee guida di sviluppo di OWASP
Il team di sviluppo ha eseguito Vulnerability Assessment/Penetration Test sull'applicazione.	Si, vengono svolte attività di VA periodiche sul software Globaleaks sia dal reparto tecnico ISWEB si da organismi esterni.
L'applicazione gode di una protezione conforme alle best practice più aggiornate, nell'archiviazione delle password.	Si, tutte la password memorizzate nel database sono criptate attraverso combinazione di algoritmi Curve25519, XSalsa20 e Poly1305. Sono inoltre presenti controlli in fase di registrazione contro l'inserimento di password deboli, e sono correttamente previste funzioni per il cambio password a scadenza temporale.
Permettiamo l'obbligo di revisione, da parte di un responsabile, dei dati inseriti dall'utente prima di procedere con l'archiviazione definitiva del dato, al fine di agevolare l'azienda cliente nel garantirsi la minimizzazione dei dati.	Non applicabile dato il contesto applicativo.
Garantiamo agli utenti dell'applicazione la possibilità	Si, attraverso gli strumenti disponibili nella

di reperire e aggiornare tutti i dati che lo riguardano, presenti nell'applicazione.	piattaforma gli utenti possono comunicare in modalità anonima e sicura con i gestori delle segnalazioni incaricati dal Committente ai fini di aggiornamento dei propri dati o di quelli della segnalazione iniziale.
I dati memorizzati nel sistema sono crittografati, al fine di proteggerli in caso di furto o fuoriuscita accidentale.	La piattaforma utilizza un protocollo di crittografia specificatamente disegnato sull'applicativo, che utilizza i seguenti metodi: ✓ Libsodium SealedBoxes, un sistema che combina gli algoritmi Curve25519, XSalsa20 e Poly1305 per la crittografia asimettrica. ✓ Libsodium SecretBoxes, un sistema che combina gli algoritmi XSalsa20 e Poly1305 per la crittografia simettrica.
I dati in transito da e verso l'applicazione sono protetti da crittografia, per proteggerli in caso di intercettazione.	Si, l'applicazione utilizza correttamente il protocollo SSL per tutte le comunicazioni in entrata ed in uscita
Le categorie di dati particolari [Art. 9 GDPR] sono pseudonimizzati nel momento dell'archiviazione, al fine di proteggere la privacy dell'individuo in caso di furto o fuoriuscita accidentale degli stessi.	Non è prevista la raccolta di dati appartenenti a categorie particolari.
Le categorie di dati particolari [Art. 9 GDPR] vengono classificati nel momento in cui vengono immessi nel nostro software e seguono un flusso totalmente distinto da altri dati personali, allo scopo di poterli identificare facilmente durante il loro percorso e permanenza all'interno dell'applicazione.	Non è prevista la raccolta di dati appartenenti a categorie particolari
L'applicazione utilizza dei sistemi per la cancellazione sicura dei dati.	Si, la piattaforma utilizza dei sistemi di cancellazione sicura per tutti i dati trattati.

3. Conclusioni

3.1 Rischio Residuale

Il servizio Whistleblowing è stato implementato con il solo scopo di mettere a disposizione del committente un ambiente sicuro per la raccolta di segnalazioni su comportamenti illeciti o di violazioni ai modelli organizzativi adottati dall'ente o azienda cliente.

Non è interesse del servizio ottenere informazioni diverse da quelle direttamente richieste.

Le categorie di dati trattati sono quindi relative a:

- Dati anagrafici semplici del segnalante, definiti dal Committente, come ad esempio:
    - Nominativo
    - Codice fiscale
    - Posizione e ruolo nell'organizzazione
    - Dati di recapito (indirizzo, telefono, email)
- Dati descrittivi della segnalazione che viene effettuata, definiti dal Committente, come ad esempio
    - Descrizione libera della segnalazione, con annotazioni sulla tipologia della stessa
    - Data e durata della condotta oggetto di segnalazione
    - Indicazione dei soggetti giuridici e fisici che possono aver commesso il fatto
    - Indicazione di altre autorità o di altri soggetti informati
    - Luogo in cui è stato commesso il fatto
    - Annotazioni libere di maggiori dettagli

Date le misure adottate, il rischio residuale quindi è da considerarsi minimo.

Contatti

ISWEB S.p.A.

Azienda certificata UNI EN ISO 9001:2015 - RINA
“Progettazione e sviluppo applicativi software per ambienti di rete”

Sede legale e factory:
Via Cadorna, n.31 - 67051 - Avezzano (AQ)
Unità locale (commerciale):
via Fiume Giallo, 3 - 00144 - Roma

NUMERO VERDE
800.97.34.34

Tel. +39.0863.441163
Fax. +39.0863.444757

e-mail: info@isweb.it
pec: pec@pec.isweb.it
Sito web: http://www.isweb.it

DICHIARAZIONE SULLE MISURE DI SICUREZZA APPLICATE SERVIZI AMBITO WHISTLEBLOWING

Data Ultimo aggiornamento:	21/10/2023

www.isweb.it

ISWEB S.p.A.
Via Tiburtina Valeria Km. 112,500
67068 Cappelle dei Marsi (AQ)
Via Fiume Giallo 3 - 00144 Roma

ISO 9001-2015 - RINA
Sistema di gestione della
qualità certificato RINA
Certificato n° 14770/06/S

Numero Verde Gratuito
800 97 34 34

Indice

Premessa

Nell'erogazione dei propri servizi, ISWEB si impegna ad osservare le misure di sicurezza che seguono, anche ai sensi della Circolare AGID 18 aprile 2017, n. 2/2017, in quanto applicabili e indicate nel presente documento. SI precisa inoltre che nell'ambito del servizio Whistleblowing, le misure di sicurezza organizzative e tecniche applicate sono conformi all'attuale D. Lgs. n. 24/2023 e relative linee guida.

Sicurezza delle piattaforme software

Sviluppo

Il servizio Whistleblowing, è basato sul software opensource Globaleaks (*https://github.com/globaleaks/GlobaLeaks*), sviluppato secondo le line guida OWASP per lo sviluppo di applicazione sicure.
Per ogni approfondimento tecnico, è disponibile un'ampia documentazione sui principi di architettura e di security applicativa utilizzati per lo sviluppo del software, all'interno della documentazione di piattaforma disponibile all'indirizzo *https://docs.globaleaks.org/en/main/*

Verifiche periodiche di vulnerabilità

Il codice della piattaforma Globaleaks è periodicamente verificato dalla stessa community nel durante del ciclo di sviluppo, e dal reparto tecnico ISWEB all'interno delle procedure di upgrade dei servizi offerti.
Il repository della piattaforma rende disponibili anche la documentazione relativa a test di vulnerabilità svolti periodicamente e realizzati da organismi indipendenti.

Patch management

Le patch di sicurezza vengono applicate con tempestività sulla base dei rilasci ufficiali nel repository di piattaforma.
Le patch che non incidono sulla sicurezza vengono rilasciate secondo la calendarizzazione del reparto tecnico, con cadenza comunque mai superiore ad un semestre.

Sicurezza dell'accesso alle piattaforme software da parte di personale ISWEB

Tracciamento degli accessi utente e utenze

ISWEB individua specificamente i propri utenti e le relative utenze abilitate agli accessi alle piattaforme che trattano dati personali dei clienti in funzione degli specifici privilegi di accesso.
Gli accessi sono configurati a livello applicativo in modo che gli utenti non possano alterare i log.

Formazione degli utenti

Gli utenti ricevono adeguata formazione in materia di sicurezza informatica e rispetto delle prescrizioni di cui alla normativa sulla protezione dei dati personali

Continuità operativa e disaster recovery

Ripristino attività a seguito di criticità della piattaforma

ISWEB utilizza i servizi di facility management di primari data-center italiani che prevedono politiche di backup e continuità operativa in grado di ripristinare la disponibilità dei dati e dei servizi entro 24 ore dalla criticità, salvi eventi di gravità tale da non consentire il rispetto del termine suindicato.

Ripristino attività a seguito di criticità dell'infrastruttura

Benché ISWEB si impegni al rispetto dei termini di cui al precedente paragrafo, in caso di criticità relativa all'infrastruttura di facility management i tempi di ripresa dell'erogazione dei servizi dipenderanno da quelli impiegati dal data-center per ritornare all'operatività.

Si precisa che soluzioni dedicate di DR sono disponibili su progetto.

Misure anti-intrusione

L'infrastruttura di facility management prevede la presenza di firewall e antivirus perimetrali.

Altre Misure di sicurezza

- ✓ Infrastruttura tecnologica di tipo VPC - Virtual Private Cloud;
- ✓ Alta capacità di elaborazione garantita da processori fisici Intel Xeon Silver;
- ✓ Storage Area Network (SAN) in fiber channel completamente ridondata;
- ✓ Sistemi avanzati di monitoraggio proattivo per le metriche di servizio;
- ✓ Firewall perimetrale con possibilità di gestione geografica dei pacchetti;
- ✓ Supporto per l'esposizione del servizio tramite rete TOR oppure tramite normale TLS;
- ✓ Autenticazione 2FA nativa basata su RFC 6238 con chiave secreta a 160 bits;
- ✓ Sistemi di Proof of Work per login e file submission;
- ✓ Disponibilità di funzionalità di Slowdown per i tentativi di login falliti;
- ✓ Gestione delle policy per la corretta getsione di Strict-Transport, Content-Security, Cross-Origin-Embedder, Cross-Origin-Resource, Cache-Control;
- ✓ Application sandboxing: AppArmor by default per una esecuzione sicura dell'applicazione;
- ✓ Network sandboxing: layer dedicato di firewall software integrato con iptables;
- ✓ Implementazione logiche applicative di DoS Resiliency;
- ✓ Crittografia applicativa dei dati con chiavi a 256 bit ed utilizzo di:
  - Crittografia asimmetrica: Libsodium SealedBoxes (Curve25519, XSalsa20, Poly1305);
  - Crittografia simmetrica: Libsodium SecretBoxes (XSalsa20, Poly1305);
- ✓ · Sistema di eliminazione sicura dei dati.

Allegato 1 – Misure minime di sicurezza ICT-PA

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Tutte le risorse attive sono censite all'interno dei repository del reparto tecnico ISWEB sia con modalità manuali sia con modalità automatiche garantite dagli apparati di rete
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Tutte le risorse attive sono censite all'interno dei repository del reparto tecnico ISWEB sia con modalità manuali sia con modalità automatiche garantite dagli apparati di rete
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	Il server DHCP effettua il log di ogni operazione all'interno della rete aziendale.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	I repository dei dispositivi sono aggiornati automaticamente ad ogni modifica
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Gli apparati di rete utilizzano modalità automatiche per il censimento dei dispositivi
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	Gli apparati di rete che censiscono i dispositivi, memorizzano anche l'indirizzo IP sia nel caso di assegnazione dinamica sia nel caso di assegnazione statica.
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	L'inventario dei dispositivi dispone di queste informazioni

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server,	Il reparto tecnico ISWEB mantiene un elenco dei software utilizzabili da ogni dispositivo in utilizzo

				workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	I sistemi sono monitorati automaticamente dai sistemi protezione software utilizzati e dal sistema operativo stesso

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Tutti I dispositivi utilizzati applicano le configurazioni di sicurezza standard
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Tutti I dispositivi utilizzati applicano le configurazioni di sicurezza standard
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Nel caso di verifica di compromissione di un sistema o di un dispositivo, si procede con un completo ripristino e con l'applicazione della configurazione standard iniziale
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Tutte le immagini di installazione utilizzate sono sempre disponibili anche offline in repository locali o su supporti fisici
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	Tutte le operazioni che richiedono una gestione remota, sono sempre eseguite tramite canali sicuri come SSH, SFTP e HTTPS
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	Sono attivi servizi di monitoraggio continuo
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	I servizi di monitoraggio producono alert e log
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del	Tutti I dispositivi utilizzano la verifica della firma digitale dei software

				sistema, delle variazioni dei permessi di file e cartelle.	tramite le funzionalità garantite dai produttori dei sistemi operativi utilizzati. Anche I software antivirus e firewall utilizzati nelle configurazioni standard effettuano un monitoraggio di questo tipo.

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	Le verifiche vengono svolte sia come procedura stessa del ciclo di sviluppo dell'applicativo Globaleaks, sia periodicamente dal nostro reparto tecnico con cadenza al massimo annuale. La piattaforma è inoltre periodicamente verificata anche da organismi indipendenti con periodicità stabilita dagli sviluppatori.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Le verifiche vengono svolte sia come procedura stessa del ciclo di sviluppo dell'applicativo Globaleaks, sia periodicamente dal nostro reparto tecnico con cadenza al massimo annuale. La piattaforma è inoltre periodicamente verificata anche da organismi indipendenti con periodicità stabilita dagli sviluppatori.
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	Tutte le attività di verifica vengono svolte dal solo personale autorizzato e con strumenti validati ed autorizzati.
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente	I software utilizzati per le verifiche vengono continuamente aggiornati con modalità sia automatiche che manuali quando necessario.

				aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	I software utilizzati per le verifiche vengono continuamente aggiornati con modalità sia automatiche che manuali quando necessario.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Tutte le postazioni utilizzano le procedure di aggiornamento automatiche previste dal sistema operativo utilizzato. Per le componenti applicative del servizio, le modalità di aggiornamento possono variare in funzione dell'applicazione stessa.
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Non sono utilizzati sistemi separate dalla rete.
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	Tutte le eventuali vulnerabilità software vengono verificate all'interno dei cicli di sviluppo del software e nelle attività di verifica interne
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	Il piano di gestione dei rischi, ed in generale lo scenario e la matrice degli utilizzatori sono stati definiti durante il design del software e vengono aggiornati sulla base di ogni modifica allo scenario (https://docs.globaleaks.org/en/main/security/index.html)

4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	Tutte le operazioni di patching e di upgrade dei software sono sempre associate alle eventuali vulnerabilità rilevate o alla segnalazione di bug.
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	Nel caso di vulnerabilità non risolvibili in tempi brevi, vengono sempre applicate misure alternative temporanee per la mitigazione della stessa fino alla risoluzione effettiva
4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	Tutti I cili di sviluppo software e le relative verifiche vengono effettuate in ambienti di collaudo separati da quelli di produzione

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Le utenze di amministrazione del servizio sono in disponibilità esclusiva al reparto tecnico ISWEB ed ai referenti individuati dal committente
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Tutti gli accessi utente, anche quelli non riusciti, vengono registrati nel log delle attività dell'applicazione e nei log di servizio. Si specifica che gli accessi amministrativi utilizzati dagli operatori ISWEB, non consentono la visualizzazione o gestione dei dati delle segnalazioni Whistleblowing, ma solo gli aspetti di configurazione dell'ambiente, utilizzati per la predisposizione dei requisiti funzionali richiesti dal committente.

5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	L'ambiente applicativo utilizza un Sistema ACL modulare per l'assegnazione dei permessi all'utente. Si specifica che gli accessi amministrativi utilizzati dagli operatori ISWEB, non consentono la visualizzazione o gestione dei dati delle segnalazioni Whistleblowing, ma solo gli aspetti di configurazione dell'ambiente, utilizzati per la predisposizione dei requisiti funzionali richiesti dal committente.
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Tutte le operazioni amministrative effettuate vengono registrate nel log delle attività dell'applicazione, che si occupa anche di registrare eventuali eccezioni o anomalie delle funzioni disponibili.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	L'ambiente applicativo dispone di una funzione dedicata alla gestione delle utenze amministrative.
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Tutti i dispositivi vengono configurati in fase iniziale secondo gli utilizzi.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Tutte le operazioni amministrative effettuate vengono registrate nel log delle attività dell'applicazione.
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Tutti gli accessi utente, sia quelli tentati che quelli riusciti, vengono registrati nel log delle attività dell'applicazione
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	L'autenticazione a due fattori è supportata ed attivabile sul servizio Whistleblowing dietro richiesta da parte del committente.
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	L'autenticazione a due fattori è supportata ed attivabile sul servizio Whistleblowing. La piattaforma supporta inoltre ulteriori regole per la costruzione di password robuste.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Le password vengono valutate in tre livelli: forte, accettabile, inutilizzabile. Una password forte deve essere

					formata da lettere maiuscole, lettere minuscole, numeri e simboli, essere lunga almeno 12 caratteri e includere una varietà di almeno 10 input diversi. Una password accettabile dovrebbe essere formata da almeno 3 input diversi su lettere maiuscole, lettere minuscole, numeri e simboli, contenere almeno 10 caratteri e includere una varietà di almeno 7 input diversi.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	La piattaforma richiede alle utenze un cambio password periodico (configurabile su richiesta)
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	L'ambiente applicativo controlla che ogni nuova password impostata non sia uguale a quella già utilizzata dall'utente
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	L'ambiente applicativo utilizza un Sistema ACL estremamente modulare per l'assegnazione dei permessi all'utente. Gli account sono sempre indipendenti sulla base dei relativi ACL.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Questo aspetto è gestito dal committente, tramite l'individuazione dei propri operatori e dei relativi account.
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	Gli accessi amministrativi a livello servizio vengono utilizzati esclusivamente quando strettamente necessario al tipo di operazioni. Le utenze di questo tipo sono assegnate esclusivamente agli AdS assegnati al relativo servizio.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le password non sono mai memorizzate in chiaro sul sistema, ma vengono memorizzate con un hash costruito da un salt randomico a 128bit e l'algoritmo Argon2
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Nel caso di utilizzo di chiave private come nel caso di attivazione di PGP, il mantenimento di queste è in carico agli AdS individuati dal committente in quanto il reparto tecnico di ISWEB non ha accesso ai datri inerenti il servizio.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	Tutte le postazioni utilizzate dispongono di software antivirus aggiornati automaticamente.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Tutte le postazioni utilizzate dispongono di software Firewall ed IPS aggiornati automaticamente con il sistema operativo. Sono anche presenti sistemi firewall hardware nella rete.
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Gli operatori ISWEB utilizzano esclusivamente dispositivi autorizzati.
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	Tutte le postazioni ed i dispositivi consentiti sono configurati con funzionalità DEP e di controllo dell'account.
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	Le funzionalità sono incluse negli strumenti software antivirus e firewall utilizzati. In termini infrastrutturali, sono garantite dagli apparati e le policy infrastrutturali.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Le funzioni sono disabilitate di default nei software utilizzati
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Le funzioni sono disabilitate di default nei software utilizzati
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Le funzioni sono disabilitate nei servizi utilizzati
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Le funzioni sono disabilitate di default nei software utilizzati
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Le funzionalità sono incluse negli strumenti software antivirus e firewall utilizzati da ogni postazione utilizzata
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Le funzioni sono incluse nei servizi utilizzati
8	9	2	M	Filtrare il contenuto del traffico web.	Le funzionalità sono incluse negli strumenti software antivirus e firewall utilizzati

8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	Le funzioni sono incluse nei servizi utilizzati e negli strumenti software antivirus e firewall utilizzati da ogni postazione
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Le funzionalità sono incluse negli strumenti software antivirus e firewall utilizzati

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Le funzionalità sono incluse nelle policy di business continuity. Inoltre le funzionalità di DR sono attivabili in modalità dedicata sul singolo progetto
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	Le informazioni riservate contenute dal servizio sono crittografate nativamente dall'ambiente applicativo.
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	I dati relativi ai backup non sono mai disponibili su servizi normalmente esposti

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	Nell'ambito del servizio Whistleblowing, l'analisi è stata effettuata già a monte del software design (https://docs.globaleaks.org/en/main/security/index.html)

13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Le funzionalità sono garantite dagli apparati firewall e dai software antivirus utilizzati.

Contatti

ISWEB S.p.A.

Azienda certificata UNI EN ISO 9001:2015 - RINA
"Progettazione e sviluppo applicativi software per ambienti di rete"

Sede legale e factory:
via Tiburtina Valeria Km. 112,500 - 67068 - Cappelle dei Marsi (AQ)
Unità locale (commerciale):
via Fiume Giallo, 3 - 00144 - Roma

NUMERO VERDE
800.97.34.34

Tel. +39.0863.441163
Fax. +39.0863.444757

e-mail: info@isweb.it
pec: pec@pec.isweb.it
Sito web: http://www.isweb.it

Registro delle Imprese di L'Aquila
P.IVA, C.F. e numero d'iscrizione: 01722270665

ISWEB CLOUD

Cloud Service Provider Certificato ACN

Data ultimo aggiornamento:	21/10/2023

ISWEB S.p.A.
Via Cadorna 31 - 67051 Avezzano (AQ)
Via Fiume Giallo 3 - 00144 Roma

www.isweb.it

ISO 9001-2015 - RINA
Sistema di gestione della qualità certificato RINA
Certificato n° 14770/06/S

Numero Verde Gratuito
800 97 34 34

INDICE

PREMESSA

Le caratteristiche dell'infrastruttura ISWEB Cloud, descritte nel presente documento sono relative sia ai servizi condivisi disponibili per tutti i nostri Clienti, sia ai servizi dedicati, rivolti a coloro che hanno specifiche esigenze e preferiscono godere dei benefici garantiti da un servizio personalizzato e da una infrastruttura completamente indipendente.

L'infrastruttura ISWEB Cloud è fornita da Seeweb S.r.l., partner affidabile da oltre un decennio, tra le prime 10 Hosting Company a livello mondiale per affidabilità e qualità del servizio (audit Netcraft), rappresenta un marchio simbolo di affidabilità, sicurezza ed elevate prestazioni. Il partner è dotato di quattro data-center di proprietà, due nella sede di Milano e due a Frosinone.

L'infrastruttura ISWEB Cloud ISWEB è certificata da ACN nell'ambito dei CSP.

Certificazioni e accreditamenti del partner Seeweb S.r.l.

Seeweb dispone dei certificati e accreditamenti elencati di seguito:

- Certificazione di processo secondo ISO9001
- Certificazione di compatibilità ambientale ISO14001
- Certificazione per l'erogazione di servizi ISO20001
- Certificazione di sicurezza dei dati ISO27001
- In possesso di verifica della compliance a ISO27017
- In possesso di verifica della compliance a ISO27018
- Registrar Accreditato presso il ccTLD Italiano e presso Eurid per il TLD .EU
- Cloud Provider accreditato presso ACN per Cloud PA
- LIR – Local Internet Registry per IPv4 e IPv6 accreditata presso RIPE NCC
- Accreditata e sottoposta ad audit di affidabilità con Netcraft Ltd
- Microsoft Partner con autorizzazione SPLA e personale MCP

Continuità operativa

I servizi tecnici offerti da ISWEB sono basati su tecnologie altamente scalabili ad elevate prestazioni volte a garantire il massimo livello di continuità operativa.
Importanza strategica ha assunto l'obbligo di definire specifiche politiche volte proprio a garantire la continuità operativa, requisito indispensabile in ambito PA.
ISWEB garantisce un uptime del 99,5% su base annua.

I CENTRI SERVIZI

I data-center dai quali sono erogati i servizi sono situati sul territorio italiano e posti ad elevata distanza tali da assicurare la completa indipendenza dei domini di disastro secondo le normative internazionali più stringenti.

Descrizione dei datacenter

Tutti i datacenter sono di proprietà e in completa gestione del fornitore.

- ✓ **SITO 1 - Milano 1**: via Caldera, 21: facility con tecnologia convenzionale (raffreddamento perimetrale under floor) ma efficienza medio alta (PUE medio stagionale c.a. 1,6); datacenter di 700mq dedicato principalmente ai servizi di colocation (shelf, rack, cage). Potenza nominale massima: 500KW. Classificazione non certificata: TIER III. Operatori presenti in datacenter: Telecom Italia, Fastweb, Wind, Cogent Communications, Level3, GTT, Mix (fibre disponibili). Sistema di rilevazione dei fumi e del fuoco EN54-7; EN54-5. Estinzione incendi a saturazione di Argon. Alimentazione Media Tensione da anello, gruppi elettorgeni di emergenza N+1.

- ✓ **SITO 2 - Milano 2**: via Caldera, 21: facility con tecnologia ad alta efficienza “in rack” (raffreddamento locale dei rack ad alta densità) efficienza alta (PUE medio stagionale c.a. 1,4); datacenter di 250mq dedicato principalmente ai servizi di cloud computing. Potenza nominale massima: 300KW. Classificazione non certificata: TIER III. Operatori presenti in datacenter: Telecom Italia, Fastweb, Wind, Cogent Communications, Level3, GTT , Mix (fibre disponibili). Sistema di rilevazione dei fumi e del fuoco tipo Vesda multiarea progressivo. Estinzione incendi a saturazione di Argon. Alimentazione Media Tensione da anello, gruppi elettrogeni di emergenza N+1.

- ✓ **SITO 3 - Frosinone 1**: C.so Lazio, 9/a: facility con tecnologia convenzionale (raffreddamento perimetrale under floor) con efficienza media (PUE medio stagionale c.a. 1,8); datacenter di 200mq dedicato ai servizi di cloud computing e, parzialmente, di colocation (shelf, rack). Potenza nominale massima: 200KW. Classificazione non certificata: TIER II+. Operatori presenti in datacenter: Telecom Italia, Fastweb, Wind, Infracom, Namex (fibre disponibili). Sistema di rilevazione dei fumi e del fuoco EN54-7; EN54-5. Estinzione incendi a CO2 e polvere. Alimentazione Bassa Tensione, gruppo elettrogeno di emergenza.

- ✓ **SITO 3 - Frosinone 2**: Via Vona, 66 (zona industriale): facility di recentissima costruzione con tecnologie innovative (raffreddamento perimetrale under floor e combinato in rack con frecooling con acqua a temperatura moderata (15-20°) e grande portata, efficienza alta (PUE medio stagionale c.a. 1,3-1,35); datacenter di 1000mq dedicato ai servizi di cloud computing e, di colocation (shelf, rack, cage). Potenza nominale massima: 1000KW. Classificazione non certificata: TIER III+ (TIER IV a livello design). Operatori presenti in datacenter: Telecom Italia, Fastweb, Wind, Infracom, Namex (fibre disponibili). Sistema di rilevazione dei fumi e del fuoco tipo Vesda multiarea progressivo. Estinzione incendi con sistema HI-FOG® di Marioff water mist ad alta pressione twin fluid secondo quanto indicato dallo standard NFPA 750 e UNI CEN/TS 14972. Alimentazione Media Tensione, gruppi elettrogeni di emergenza N+1.

Sistemi e procedure di sicurezza

Per tutti i centri sono garantite le condizioni climatiche secondo raccomandazioni ASHRAE 2008.
Per tutti i datacenter sono disponibili sistemi di controllo accessi, rilevamento intrusioni, videosorveglianza conformi alle norme: CEI EN 50131 allarmi antifurto - CEI EN 50132 tvcc - CEI EN 50133 controllo accessi - CEI EN 50134 allarmi sociali - CEI EN 50136 trasmissione di allarmi - EN 50137 sistemi integrati di allarme - EN50118 centrali di ricezione/telesorveglianza.

MISURE FISICHE E AMBIENTALI

a. Accesso ai locali

L'accesso ai Datacenter è riservato esclusivamente ai dipendenti della società Seeweb ed a personale terzo opportunamente autorizzato ed è condizionato all'accesso alla sede Seeweb possibile a mezzo protetto da Badge/Secret di riconoscimento. L'accesso all'area di Datacenter è ulteriormente subordinato ad autorizzazione a mezzo SmartCard/Secret in possesso del solo personale autorizzato alle attività di datacenter. Il Datacenter A dispone di controllo accessi a tecnologia biometrica combinata con acquisizione del volto del richiedente l'accesso. Tutti gli accessi sono sottoposti a logging su sistema informatico, eventuali terzi che accedono unicamente accompagnati da personale interno vengono registrati previo accertamento dell'identità e verifica della motivazione/autorizzazione all'accesso. Ogni autorizzazione concessa è valida per un solo periodo di accesso.

b. Sorveglianza del locali

È assicurata la sorveglianza dei locali 365/7/24 con personale proprio e/o esterno autorizzato e con sistemi di monitoraggio remotizzato. Esiste una videosorveglianza perimetrale esterna e interna a mezzo telecamere con registrazione e ritenzione a norma di legge con rilevazione dei movimenti in aree critiche e conseguente attivazione di circuito di allarme. La videosorveglianza con registrazione e ritenzione è presente anche all'interno dei locali operativi e tecnici dei DC. Nel sito 4) è presente una sorveglianza armata dedicata nelle ore di minore frequentazione; nei siti 1) e 2) la sorveglianza armata è condivisa a livello di campus.

c. Rilevamento intrusioni

È presente un sistema di rilevazione delle intrusioni a monitoraggio degli accessi sui varchi e di tipo volumetrico per tutti i locali della sede e del Datacenter con segnalazione locale ti tipo ottico/acustico locale e remota a mezzo radio allarme verso istituto di vigilanza. Tutti i varchi critici sono allarmanti e a rilevazione di stato, le informazioni sono archiviate e non modificabili. Il sito 4) è protetto anche da perimetrale esterno attraverso barriere a microonde coordinato con il sistema di controllo degli accessi e di videosorveglianza.

d. Infrastruttura fisica di rete

L'infrastruttura di rete all'interno del datacenter è a tre livelli, completamente ridondata negli apparati coinvolti e nei collegamenti fino al rack di utilizzo. I livelli di backbone e di aggregazione sono allocati in un'apposita area del datacenter e opportunamente protetti, il livello di distribuzione è locale alla singola fila di rack. Entrambi i collegamenti facenti parte della coppia in ridondanza sono sempre attivi e monitorati nel funzionamento. Per i datacenter tutti i percorsi rame e fibra dell'infrastruttura di rete del bundle di ridondanza sono su percorsi fisici separati e compartimentati.

e. Eventi accidentali e catastrofici

Il datacenter 4) è protetto da un sistema di rilevazione dei fumi e del fuoco tipo Vesda multiarea progressivo. Estinzione incendi con sistema HI-FOG® di Marioff water mist ad alta pressione twin fluid secondo quanto indicato dallo standard NFPA 750 e UNI CEN/TS 14972. Si tratta di un sistema particolarmente sofisticato che consente la coesistenza di operatori in campo mentre è in atto il processo di estinzione dell'incendio consentendo di ridurre al minimo l'impatto sui servizi erogati. I datacenter 1), 2) sono protetti con sistema di rilevazione dei fumi e del fuoco EN54-7; EN54-5. Estinzione incendi a saturazione ambientale con gas Argon. Rilevazione di allagamento attraverso opportuni sensori installati nel sottopavimento; i datacenter sono tutti situati al di sopra del piano campagna, molto oltre i livelli di piena storici e comunque esiste un sistema di percolazione a protezione di eventuali perdite di acqua degli impianti di refrigerazione che è l'unica possibile causa di allagamento.

f. Continuità dell'alimentazione

Il Sistema di alimentazione è completamente ridondante su doppia linea a norme EIE-CE per ogni fila di armadi con prese e spine di sicurezza antistrappo e antifuoco. Ogni armadio contenente le apparecchiature riceve l'alimentazione da due diverse linee provenienti da UPS ridondati. Il datacenter 4) dispone di un design elettrico full TIER-IV con doppio UPS e doppio STS sulle linee di alimentazione delle utenze (rack) con percorsi elettrici doppi, separati e compartimentati. I siti sono dotati di gruppi elettrogeni ad avvio automatico a lunga autonomia (72h per il sito 4); 24h per i siti 1), 2), 3) a pieno carico) con possibilità di rifornimento rapido a piano strada. Il sito 4) dispone di un sistema di generazione di emergenza N+1 capace di operare anche in servizio continuativo in luogo dell'alimentazione da rete pubblica.

g. Condizionamento dei locali

Il sistema di condizionamento provvede alla filtrazione dell'aria, alla ventilazione interna ed al raffreddamento garantendo quindi la giusta temperatura ed il sufficiente ricambio d'aria. L'impianto di condizionamento è ridondato secondo un'architettura completamente protetta di tipo 2N+1 estesa ai gruppi refrigeranti ad acqua, ai condensatori esterni e alle unità di trattamento aria (UTA) presenti nel datacenter. Il sistema non protetto (con una avaria in corso) presenta un sovradimensionamento del 20% rispetto alla capacità massima dell'area di datacenter servita. In caso di avaria totale è stato previsto un sistema di lavaggio dell'aria tramite immissione/espulsione dell'aria esterna (freecooling) ad azionamento manuale. I parametri di esercizio sono costantemente misurati in passi da 5 minuti con allarmi locali e remoti (teleallarmi su istituto di vigilanza) al superamenti di valori critici. L'impianto garantisce il mantenimento dei parametri secondo la raccomandazione ASRHAE 2008 classe A degradando al più ad A1 in caso di avaria.

Infrastruttura

INFRASTRUTTURA DI RETE

I servizi di presenza su Internet non possono prescindere da una infrastruttura di rete che offra adeguate performance e un elevato grado di ridondanza in modo da assicurare un servizio continuativo e con un elevato standard di qualità.

Il partner dispone di una propria backbone proprietaria che collega attraverso un anello interamente in Fibra ottica i propri Data-center e il Pop di Roma Namex, la tecnologia della connessione è DWDM con grande capacità disponibile. Ogni sede di datacenter di Seeweb ed il Pop di Roma Namex sono dotati di infrastruttura completamente ridondata a livello di border router e di core switch consentendo la tolleranza ai guasti dei componenti e la manutenzione online senza fermo dei dispositivi core della rete.

Seeweb è LIR Local Internet Registry accreditato presso il RIPE-NCC con allocazioni IPv4 e IPv6.

L'infrastruttura attualmente acquisisce risorse da:

- NTT Communications – Milan, 10 Gbps
- GTT Communications – Milan. 10 Gbps
- GTT Communications – Rome, 10 Gbps
- Cogent Communications – Milan, 10 Gbps
- TIM Telecom Italia – Milan, 4 Gbps
- TIM Telecom Italia – Rome. 4 Gbps
- Swisscom – Lugano (CH), 1Gbps
- Cogent Communications – Zagreb (HR), 10 Gbps

È presente presso i seguenti punti di interscambio neutrali presso i quali attua politiche di open peering tese all'ottenimento dei migliori indici possibili di qualità, latenza e prestazioni:

- MIX - Milan, 10 Gbps
- NAMEX - Rome, 10 Gbps
- MINAP - Milan, 10 Gbps
- AMSIX - Amsterdam, 1 Gbps
- AMSIX - Amsterdam, 5 Gbps
- CIX – Zagreb (HR), 10Gbps
- SIX – Lubiana, 1 Gbps

Il partner dispone di Autonomous System AS12637 tramite accordi con i fornitori di transito IP che consentono di effettuare operazioni di ingegneria BPG sia per garantire la migliore qualità possibile delle connessioni sia per agire tempestivamente con tecniche di mitigazione in caso di dDoS o situazioni critiche della rete.

Su tutta la rete è già implementato e in produzione il nuovo protocollo Ipv6.

INTERCONNESSIONE CON LA RETE DELLE PUBBLICHE AMMINISTRAZIONI SPC – QXN

Sui punti d'interscambio di Mix (Milano) e Namex (Roma) è possibile interconnettere la rete della pubblica amministrazione SPC – QXN.
Il sistema di rete, con la sola eccezione del collegamento verso il punto di interscambio di Amsterdam AmsIX è tale per cui ogni percorso è ridondato, anche a livello di percorso fibra fisico. È pertanto in grado di tollerare, senza degrado nelle prestazioni il guasto dei circuiti geografici in fibra ottica e questo consente di remotare in sicurezza anche le connessioni con SPC nell'ambito della propria backbone e dei propri centri servizi e POP
La connessione a SPC – QNX può essere realizzata, a seconda delle scelte e delle policy, anche in modalità multipla:

- Presso il datacenter Seeweb di Milano
- Presso il datacenter Seeweb di Frosinone
- Presso il Mix di Milano (sede QXN), attraverso nostre risorse di trasporto
- Presso il Namex di Roma (sede QXN), attraverso nostre risorse di trasporto

Il collegamento può essere effettuato in doppia via (per es. a Roma e a Milano da definire se presso i Datacenter di esercizio e disaster recovery ovvero direttamente presso i punti i presenza di SPC prezzo Namex e Mix).

INFRASTRUTTURA SERVER

Le apparecchiature che sovrintendono all'erogazione dei servizi sono realizzate su hardware di classe enterprise utilizzando server fisici multiprocessore ridondati N+1. I vendor e le tipologie di apparati in uso attualmente sono:

- IBM BladeCenter con Blade HS23 dotate di processori Intel(R) Xeon(R) CPU E5-2640 v2 @ 2.00GHz
- HP Blade con Blade ProLiant BL460c Gen8 dotate di processori Intel(R) Xeon(R) CPU E5-2640 v2 @ 2.00GHz

Il partner garantisce che le eventuali evoluzioni dell'infrastruttura hardware in corso d'opera saranno tali da mantenere inalterate, ovvero migliorate le prestazioni minime indicate.

SOTTOINSIEMI DI STORAGE

Il sottosistema di storage è di tipo SAN – Storage Area Network in tecnologia fiber channel a 8 e 4Gbps, tutti i sistemi sono dotati di cablaggi in fibra ottica con topologia di tipo multipath. Gli apparati in uso sono:

- IBM XIV Storage System nei tagli di capacità di 27TB, 76TB e 180TB
- Switch SANBox Qlogic e Brocade

Storage SAN IBM XIV Gen3

Si tratta di un sistema di storage di fascia alta che soddisfa l'esigenza di prestazioni, disponibilità, flessibilità operativa e sicurezza, tenendo al contempo al minimo costi e complessità.
Progettato per garantire prestazioni uniformi di fascia enterprise e disponibilità, lo storage XIV gestisce carichi di lavoro statici e dinamici con la massima semplicità, e grazie all'architettura GRID, assicura un massiccio parallelismo, che consente l'allocazione sempre uniforme delle risorse di sistema, senza mai compromettere le prestazioni a vantaggio dell'affidabilità.

Possiamo quindi riassumere le caratteristiche principali del sistema nel seguente modo:

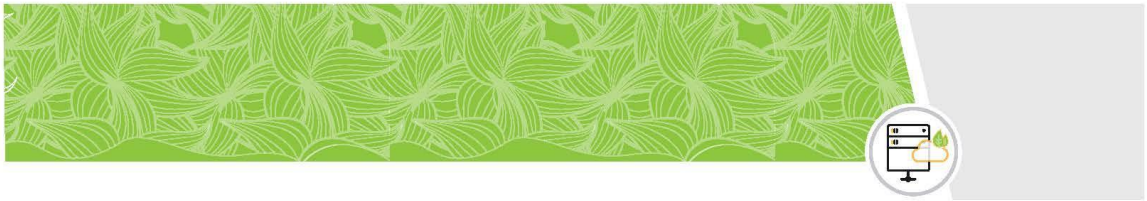
- Massiccio parallelismo in un'architettura interamente distribuita: il sistema XIV utilizza un'architettura distribuita di moduli interconnessi, ciascuno con una propria CPU multi-core, ampia cache e unità disco ad alta densità, operanti in parallelo, per fornire i dati alle applicazioni client con la massima efficienza. Ogni volume di dati viene distribuito su tutti i moduli e i dischi presenti nel sistema in modo casuale e la potenza aggregata dell'intero sistema risulta costantemente disponibile per tutte le applicazioni. Il sistema XIV presenta questo insieme di dischi come un unico archivio dati elastico di grandi dimensioni, disponibile sulla rete storage.
- Dati distribuiti: il sistema archivia i dati scomponendoli in blocchi da 1 MB denominati partizioni, tutti in mirroring tra di loro a scopo di ridondanza. Distribuisce inoltre tutte le partizioni in modo automatico e uniforme su tutti i dischi mediante un sofisticato algoritmo di distribuzione pseudo-casuale.
- Cache distribuita: l'implementazione di una cache potente e flessibile consente al sistema XIV di sfruttare ampi slot per le letture, gestendo al contempo slot di dimensioni inferiori, per garantire un eccezionale rapporto di hit della cache e, di conseguenza, prestazioni migliori.
- Larghezza di banda distribuita all'interno dei moduli: l'ampia larghezza di banda da cache a disco disponibile in ciascun modulo, insieme all'ampissima larghezza di banda aggregata di interconnettività dei moduli disponibile sul backplane XIV, consente un massiccio prefetching.
- Scalabilità intelligente: qualsiasi incremento di capacità, determinato dall'aggiunta di moduli disco, è accompagnato da un corrispondente incremento di potenza di elaborazione, cache, e connettività, per garantire livelli prestazionali sempre elevati in caso di espansione del sistema.

GDPR 679/2016 COMPLIANCE

Il Principio di Accountability (art. 24 GDPR) del GDPR chiede di dimostrare di aver adempiuto alle richieste normative. L'adesione a un codice di condotta approvato (ex art. 40 GDPR) o a un meccanismo di certificazione approvato (ex art. 42 GDPR) possono essere utilizzate per dimostrare la conformità ai requisiti. In particolare, nel 2016 Seeweb ha fondato – insieme a altri provider – il CISPE Code of Conduct. Anticipando le tematiche e le novità del GDPR. Tutti i servizi Cloud dichiarati CISPE compliant sono di per sé GDPR compliant.

Per ogni approfondimento si rimanda al codice di condotta CISPE -https://cispe.cloud- disponibile all'indirizzo https://www.codeofconduct.cloud/.

CERTIFICAZIONE DNSH



seeweb
THINK CLOUD

Conformità di Seeweb al principio DNSH (Do No Significant Harm)

Premessa
Oggi le amministrazioni devono andare nella direzione di scelte e misure che dimostrino di non arrecare danni significativi all'ambiente e ai nuovi target ambientali.
In particolare, secondo il Dispositivo per la ripresa e la resilienza (Regolamento UE 241/2021), tutte le misure dei Piani nazionali (PNRR) devono soddisfare il principio di "non arrecare danno significativo agli obiettivi ambientali". Tale vincolo si traduce in una valutazione di conformità degli interventi al principio del **"Do No Significant Harm" (DNSH)**, il cui obiettivo è valutare se una misura possa o meno arrecare un danno ai sei obiettivi ambientali individuati nel Green Deal europeo.

DNSH e Data Center
Il contesto attuale vede le amministrazioni chiamate ad accelerare i processi di digitalizzazione e, contestualmente, a investire in modo sostenibile, coerentemente con quanto riportato nelle valutazioni DNSH.
E se i Data Center sono luoghi di erogazione di servizi indispensabili per la trasformazione digitale, è vero anche che sono estremamente energivori: è quindi necessario che siano progettati in modo da contribuire al massimo agli obiettivi di miglioramento climatico.

Conformità di Seeweb al principio del DNSH
Al fine di attestare il possesso dei requisiti ambientali DNSH (Do No Significant Harm), Seeweb, impegnata sin dalla sua nascita nel monitoraggio delle emissioni e nella scelta di processi sostenibili, dichiara che:

- non arreca danno significativo all'ambiente;
- dispone della certificazione ambientale ISO14001 n.IT18-27703B, con particolare riferimento ai data center e ai processi di "Progettazione e fornitura servizi di Cloud Computing e Cloud Storage. Hosting, Housing e Colocation, Posta Elettronica, Domini Internet, Sicurezza Informatica e Disaster Recovery";
- le nuove apparecchiature IT acquisite per i data center che ospitano servizi di hosting e cloud sono certificate secondo lo standard internazionale sull'efficienza energetica Energy Star, o equivalente, secondo le norme EPA ENERGY STAR - ISO/IEC 30134-4:2017;
- i data center che ospitano i servizi di hosting e cloud prevedono un piano di gestione dei rifiuti in linea con la norma LCA – EN50625;
- dispone della certificazione che attesta che i refrigeranti utilizzati nei sistemi di raffreddamento dei data center che ospitano i servizi di hosting e cloud sono conformi al Regolamento (UE) n. 517/2014 del Parlamento Europeo e del consiglio del 16 aprile 2014 sui gas fluorurati a effetto serra, che abroga il regolamento (CE) n. 842/2006;
- dispone della certificazione delle apparecchiature dei data center in conformità con la direttiva sulla restrizione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche (EU) 2011/65.

Inoltre, in aggiunta a quanto previsto da DNSH, Seeweb ha dichiarato l'impegno a usare solo energia certificata rinnovabile per l'alimentazione dei suoi data center.

Frosinone, 4 maggio 2022

Luogo e data

Firma dell'Amministratore Delegato
Antonio Domenico Baldassarra

CONTATTI

Azienda certificata UNI EN ISO 9001:2015 - RINA
"Progettazione e sviluppo applicativi software per ambienti di rete"

Sede legale e factory:
Via Cadorna, n.31 - 67051 - Avezzano (AQ)
Unità locale (commerciale):
via Fiume Giallo, 3 - 00144 - Roma

NUMERO VERDE
800.97.34.34

Tel. +39.0863.441163
Fax. +39.0863.444757

e-mail: info@isweb.it
pec: pec@pec.isweb.it
Sito web: http://www.isweb.it

Registro delle Imprese del Gran Sasso d'Italia.
P.IVA, C.F. e numero d'iscrizione: 01722270665

whistleblowing

La soluzione applicativa per la gestione delle **segnalazioni**
sempre in linea con la normativa

Configurazione del form di segnalazione

isweb
www.isweb.it

ISWEB S.p.A.
Via Cadorna 31 - 67051 Avezzano (AQ)
Via Fiume Giallo 3 - 00144 Roma

ISO 9001-2015 - RINA
Sistema di gestione della
qualità certificato RINA
Certificato n° 14770/06/S

Numero Verde Gratuito
800 97 34 34

Indice

Home page informativa

Di seguito viene presentata la homepage pubblica del servizio, in cui vengono presentate le principali informazioni sul suo utilizzo.

Questo il testo di default per il quale è possibile richiedere la personalizzazione:

Il whistleblowing è la segnalazione effettuata da un soggetto che, nel contesto lavorativo pubblico o privato, viene a conoscenza di violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrita' dell'amministrazione pubblica o dell'ente privato. Il Dlgs 24/2023 prevede che i soggetti del settore pubblico e del settore privato attivino propri canali di segnalazione che garantiscano la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione. La soluzione applicativa adottata è pienamente conforme alle disposizioni in materia di whistleblowing.

Se devi segnalare una ritorsione subita a seguito di una segnalazione precedentemente effettuata, la comunicazione deve essere inviata esclusivamente ad ANAC tramite le modalità previste e disponibili sul sito web dell'Autorità.

Sei a conoscenza di illeciti o di qualunque informazione relativa a comportamenti scorretti nel tuo ambito di lavoro?
Invia una segnalazione (pulsante di invio)
Hai già effettuato una segnalazione?
Inserisci la tua ricevuta.

Nota: *il committente può indicare le eventuali modifiche da apportare alle informazioni della home page nel campo sottostante.*

Digitare nell'area sottostante il nuovo testo da inserire

Invio della segnalazione – Informazioni all'utente

Nel momento in cui un utente avvia l'inoltro di una segnalazione dalla pagina iniziale, il sistema presenta alcune informazioni relative alla compilazione dei propri dati anagrafici.
Come per la pagina informativa iniziale, anche in questo caso il testo può essere personalizzato sulla base delle necessità del committente.

Questo il testo di default:

> **Informazioni**
> Il conferimento dei dati personali è facoltativo, e gli eventuali dati inseriti saranno trattati per la durata della gestione della segnalazione e conservati per il tempo necessario al trattamento della stessa, e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del Dlgs 24/2023 e del principio di cui agli articoli 5, paragrafo 1, lettera e), del regolamento (UE) 2016/679 e 3, comma 1, lettera e), del decreto legislativo n. 51 del 2018. I dati saranno trattati esclusivamente dagli incaricati designati dal Titolare e da soggetti espressamente designati come Responsabili del Trattamento esclusivamente per esigenze di manutenzione tecnologica della piattaforma. I dati non saranno comunicati a terzi né diffusi, se non nei casi specificamente previsti dal diritto nazionale o dell'Unione europea.

***Nota:** il committente può indicare le eventuali modifiche da apportare all'informativa di default nel campo sottostante.*

Digitare nell'area sottostante il nuovo testo da inserire

Struttura del form di segnalazione

Di seguito viene presentata la struttura del form di segnalazione default implementato sul servizio Whistleblowing.
Il modulo di invio utilizza un raggruppamento a step delle informazioni da inserire, al fine di massimizzare l'usabilità delle interfacce di compilazione dei dati.

Di seguito andremo ad evidenziare i campi che compongono la segnalazione, al fine di permettere l'indicazione

Nota: *il committente può indicare le eventuali modifiche da apportare al modulo direttamente in questo documento, individuando le modifiche strutturali da apportare alla base dati informativa della procedura di segnalazione. Si fa presente che il documento potrebbe differire dall'eventuale prototipo di servizio attivato per il committente, nel caso siano già state attivate delle particolari configurazioni iniziali.*

Per la compilazione, è possibile sia utilizzare le aree box editabili in ogni campo del modulo, sia agire direttamente sul testo che descrive le caratteristiche del campo.

Nota: *Tutti i campi contrassegnati con l'asterisco sono obbligatori.*

STEP 1 - Segnalazione

Informazioni sulla tua segnalazione

Hai già effettuato la segnalazione ma hai perso il tuo key code? *
Valori di scelta attualmente disponibili:
- SI
- NO

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Relazione del segnalante all'epoca dei fatti *
Inserire una delle seguenti opzioni alternative fra loro:
Valori di scelta attualmente disponibili:
- Dipendente della Società
- Dipendente o collaboratore della Società con rapporto di lavoro non in vigore
- Lavoratore autonomo che svolge la propria attività lavorativa presso la Società
- Volontario o tirocinante
- Azionista
- Persone con funzioni di Amministrazione, Direzione, Controllo, Vigilanza o Rappresentanza
- Altro

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

***Nota:** Questo blocco viene visualizzato solamente nel caso di risposta precedente sul valore **SI.** Questo blocco inoltre permette l'inserimento multiplo delle informazioni.*

[ALTRO] Specificare altra relazione con l'Ente o Organizzazione
Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Tipologia di condotta illecita *
Seleziona una o più voci tra quelle presenti
Valori di scelta attualmente disponibili :

- Condotte illecite rilevanti ai sensi del d.lgs. n. 231/2001
- Violazioni dei modelli di organizzazione e gestione previsti nel d.lgs. n. 231/2001
- Illeciti penali, amministrativi, civili e contabili che rientrano nel diritto UE
- Atti od omissioni regolari o irregolari che vanificano l'oggetto o la finalità del diritto UE
- Atti od omissioni regolari o irregolari volte ad ottenere vantaggi fiscali
- Atti od omissioni riguardanti il mercato interno, che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali (art. 26, paragrafo 2, del TFUE).
- Altro

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Valori di scelta attualmente disponibili: Testo libero

[ALTRO] Specificare altra condotta illecita

Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Indica le circostanze di tempo e di luogo in cui si è verificato il fatto *

Indica il periodo (se possibile la data) e il luogo in cui si sono verificati i fatti oggetto della segnalazione.

Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Durata della condotta illecita *

Inserire le seguenti opzioni, alternative fra loro

Valori di scelta attualmente disponibili:

- La condotta illecita si è conclusa
- La condotta illecita è ancora in corso
- La condotta illecita si verifica ripetutamente
- Illecito non ancora commesso ma è verosimile che lo sarà

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

Soggetti coinvolti nei fatti

Indica chi sono i soggetti coinvolti nell'accaduto a qualunque titolo, aggiungendo tutti i dettagli che ritieni possano essere utili per finalità di verifica e indagine.

***Nota:** Questo blocco permette l'inserimento multiplo delle informazioni. Se l'utente desiderasse inserire più soggetti, può cliccare sul pulsante "Inserisci altri soggetti coinvolti". Il sistema genererà tanti blocchi quanti saranno i soggetti che l'utente intende inserire.*

Persona fisica/giuridica*

Valori di scelta attualmente disponibili:

- persona fisica
- persona giuridica

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

Nome e Cognome / Ragione sociale*

Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

Contatti
Valori di scelta attualmente disponibili: Testo libero

Se persona fisica, indicare l'amministrazione, ente o azienda per cui o con cui lavora il soggetto coinvolto
Indicare l'Ente o l'Azienda per cui o con cui lavora il soggetto indicato
Valori di scelta attualmente disponibili: Testo libero

Ruolo del soggetto nell'accaduto
Valori di scelta attualmente disponibili: Testo libero
Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

Il soggetto ha tratto beneficio dall'accaduto?
Valori di scelta attualmente disponibili:
- SI
- NO

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

A tuo avviso possiamo contattare il soggetto per richiedere ulteriori informazioni, senza pregiudicare la riservatezza della verifica della segnalazione?
Valori di scelta attualmente disponibili:
- SI
- NO

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

Descrizione dei fatti*
Descrivere quello che è successo
Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

Puoi fornirci informazioni utili per verificare la tua segnalazione?
Se fornirai informazioni e istruzioni dettagliate per coadiuvare la nostra attività di verifica della segnalazione, sarà più veloce e facile potere intervenire
Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

STEP 2 – Altri soggetti informati

Hai segnalato l'accaduto ad altra Autorità o Istituzione?*
Valori di scelta attualmente disponibili:
- SI
- NO

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Segnalazione ad Altra Autorità o istituzione

***Nota:** Questo blocco viene visualizzato solamente nel caso di risposta precedente sul valore **SI.** Questo blocco inoltre permette l'inserimento multiplo delle informazioni.*

A quale autorità o istituzione ti sei già rivolto
Valori di scelta attualmente disponibili:
- Corte dei Conti
- Autorità Giudiziaria
- Polizia
- Carabinieri
- Guardia di Finanza
- Ispettorato per la funzione pubblica
- Altra forza di polizia
- ANAC

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Note
Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

STEP 3 – Identità

Nota: *Questo blocco non è normalmente modificabile, ma è sostituibile con una struttura a scelta del committente. Relativamente ai dati anagrafici, si precisa inoltre che la richiesta può essere facoltativa (come nella configurazione standard proposta) oppure resa obbligatoria.*

Inserire nell'area sottostante eventuali variazioni per lo step dedicato all'identità

Testo per identità negata (click su "NO")

Stai effettuando una segnalazione anonima. Sarà possibile dichiarare la tua identità in seguito. In caso di identificazione arai protetto dalle tutele previste nel D.lgs 24/2023 tali per cui la tua identità e qualsiasi altra informazione da cui questa può evincersi, direttamente o indirettamente, non possono essere rivelate, senza il tuo consenso espresso, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati ai sensi degli articoli 29 e 32, paragrafo 4, del regolamento (UE) 2016/679 e dell'articolo 2-quaterdecies del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

STEP 4 – Allegati

Inserimento allegati

Allega eventuali documenti o files multimediali che documentano e comprovano i fatti segnalati

Aggiungi file

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

STEP 5 – Ulteriori informazioni

Con quali modalità sei venuto a conoscenza del fatto?
Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Puoi indicare altri soggetti che possono riferire sul fatto?*
Valori di scelta attualmente disponibili:

- SI
- NO

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Altri soggetti che possono riferire sul fatto

***Nota:** Questo blocco viene visualizzato solamente nel caso di risposta precedente sul valore **SI.** Questo blocco inoltre permette l'inserimento multiplo delle informazioni.*

Nome e Cognome
Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

Contatti
Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

Note
Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà,Valori di scelta, etc)

Hai parlato con qualcuno dell'accaduto?*

Valori di scelta attualmente disponibili:

- SI
- NO

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Altre persone a conoscenza dell'accaduto

***Nota:** Questo blocco viene visualizzato solamente nel caso di risposta precedente sul valore **SI.** Questo blocco inoltre permette l'inserimento multiplo delle informazioni.*

Valori di scelta attualmente disponibili:

- Colleghi
- Famiglia
- Sindacato
- Amici
- Il mio superiore
- Avvocato
- Altre autorità
- Altro

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Ci sono persone operanti all'interno del tuo medesimo contesto lavorativo che ti hanno assistito nel processo di segnalazione?

Le persone che ti hanno assistito nel processo di segnalazione saranno soggette alle medesime tutele previste per la tua persona, come indicato nel D.lgs 24/2023.

Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

STEP 6 – Invia

Termini di servizio*

Grazie al tuo contributo possiamo rendere l'Amministrazione più efficiente e giusta! Entro 7 giorni troverai evidenza in piattaforma del ricevimento della segnalazione. Entro tre mesi da quella data riceverai riscontro alla segnalazione. Ricorda di memorizzare il codice di 16 numeri di accesso alla tua segnalazione che ti verrà fornito dopo avere cliccato Invia. Attenzione! Non esiste altro sistema per accedere nuovamente alla segnalazione. Non sarà possibile, in alcun modo, recuperare detto codice. La norma assicura l'assoluta riservatezza dell'identità del segnalante. Non potrà, per nessun motivo, essere rivelata l'identità del soggetto che segnala atti discriminatori senza il suo consenso espresso e, nell'ambito del procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 del c.p.p.. La segnalazione è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, nonché dagli articoli 5 e seguenti del decreto legislativo 14 marzo 2013, n. 33.
Per conoscere le modalità di gestione delle segnalazioni, della trasmissione delle informazioni, del trattamento e della conservazione dei dati personali ti invitiamo a visionare l'apposita procedura sul sito dell'amministrazione.

[Link a termini di servizio aggiuntivi (sito web Organizzazione, download documento, ...)]

☒Si, ho preso visone dei termini di servizio.

Valori di scelta attualmente disponibili: Testo libero

Inserire nell'area sottostante eventuali variazioni per il campo (Label, Obbligatorietà, Valori di scelta, etc)

Contatti

Azienda certificata UNI EN ISO 9001:2015 - RINA
"Progettazione e sviluppo applicativi software per ambienti di rete"

Sede legale e factory:
via Tiburtina Valeria Km. 112,500 - 67068 - Cappelle dei Marsi (AQ)
Unità locale (commerciale):
via Fiume Giallo, 3 - 00144 - Roma

NUMERO VERDE
800.97.34.34

Tel. +39.0863.441163
Fax. +39.0863.444757

e-mail: info@isweb.it
pec: pec@pec.isweb.it
Sito web: http://www.isweb.it