

**REGOLAMENTO SULLA GESTIONE DI
SEGNALAZIONI DI CONDOTTE ILLECITE
(c.d. “WHISTLEBLOWING”)**

Aggiornato con determina amministratore unico di Venis del
10/07/2023

ART. 1 AMBITO DI APPLICAZIONE OGGETTIVO

Il presente regolamento costituisce un atto organizzativo di Venis teso a definire la procedura per la presentazione, la ricezione e la gestione delle segnalazioni delle violazioni da parte di coloro che ne sono venuti a conoscenza in un contesto lavorativo pubblico o privato che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, come disciplinato da:

- Il D.Lgs. n. 24 del 10/03/2023, che recepisce nel nostro ordinamento la direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23/10/2019, riguardante la protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea (cd. direttiva whistleblowing).
- la Legge n. 179/2017, avente ad oggetto le "Disposizioni per la tutela degli autori di segnalazioni o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato" di cui il suddetto Decreto ha abrogato solo l'art. 3;
- le Linee guida impartite dall'ANAC con delibera numero 469 del 9 giugno 2021;
- il Modello 231, il Piano anticorruzione e trasparenza e il codice etico e disciplinare di Venis S.p.A..

Sono esclusi dall'ambito di applicazione della nuova disciplina (art. 1 D.Lgs. 24/23), in particolare, le contestazioni o rivendicazioni di carattere personale nei rapporti individuali di lavoro o di impiego pubblico e le segnalazioni di violazioni in materia di sicurezza nazionale o di appalti relativi ad aspetti di difesa o sicurezza nazionale, salvo che tali aspetti siano riconducibili al diritto unionale.

La nuova disciplina prevede 3 diversi canali di segnalazione (interno, esterno e tramite divulgazione pubblica) che potranno essere utilizzati, al verificarsi di determinate condizioni, in via progressiva e sussidiaria.

ART. 2 AMBITO DI APPLICAZIONE SOGGETTIVO

L'articolo 3 del D.Lgs. 24/23 individua quali soggetti interessati dalla tutela per la segnalazione degli illeciti (in quanto suscettibili di eventuali atti ritorsivi) tutti coloro che, nel settore privato come in quello pubblico, forniscono prestazioni a favore di terzi a qualsiasi titolo, a prescindere dalla natura di tali attività, anche in assenza di corrispettivo.

La platea dei soggetti disegnata dai commi 3 e 4 dell'art. 3 del D.Lgs. 24/23 è, infatti, la più ampia possibile: **tutti i dipendenti pubblici e i lavoratori subordinati, i lavoratori autonomi e collaboratori che svolgono la propria attività presso i soggetti pubblici e privati oppure forniscono beni o servizi; liberi professionisti e consulenti, ma anche volontari e tirocinanti anche non retribuiti.** Infine la tutela si estende agli **azionisti e alle persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza**, anche laddove tali ruoli siano esercitati in via di mero fatto.

Soggetti tutti che vengono a conoscenza di condotte illecite nel loro contesto lavorativo.

Inoltre l'ambito della tutela nei confronti di tali soggetti, nella triplice forma di tutela della riservatezza, tutela contro le ritorsioni e previsioni di cause di esclusione della responsabilità, deve essere assicurata anche quando il rapporto di lavoro non sia ancora iniziato, durante il periodo di prova o successivamente allo scioglimento del rapporto purché le informazioni siano state acquisite nel corso del rapporto stesso o durante il processo di selezione.

Inoltre rileva l'ulteriore allargamento del perimetro dei soggetti che beneficiano della protezione -sempre con l'obiettivo di agevolare e incentivare l'attività del segnalatore riducendone il timore di ritorsioni e responsabilità- che arriva a ricomprendere i "facilitatori", coloro che assistono il segnalante nel processo di segnalazione, alle persone legate ad essi da uno stabile legame affettivo o di parentela e ai colleghi di lavoro che operano all'interno del medesimo contesto lavorativo del segnalante ma anche agli enti di proprietà del segnalante o in cui il segnalante lavora.

ART. 3 CONTENUTO DELLA SEGNALAZIONE

L'oggetto della segnalazione potrà riguardare **non solo violazioni effettive o potenziali della normativa europea** in determinati settori, **ma anche violazioni della normativa nazionale e regolamentare.** Nella definizione di violazioni vanno ricompresi non solo i comportamenti ma anche atti e omissioni o

informazioni per i quali il segnalante abbia fondati sospetti che possano concretizzare violazioni, supportati da elementi concreti.

Viene infine introdotta una clausola di salvaguardia generale in favore delle disposizioni di procedura penale e di quelle sulle prerogative sindacali dei lavoratori e sulla repressione delle condotte antisindacali, di cui all'art. 28 della L. 20/05/1970, n. 300.

Costituiscono condotte illecite passibili di segnalazione anche le violazioni delle misure di prevenzione previste dal Piano triennale per la prevenzione della corruzione e per la trasparenza (PTPCT) di Venis.

La segnalazione effettuata nelle forme e secondo le presenti indicazioni non sostituisce, laddove ne ricorrano i presupposti, la denuncia dei fatti all'autorità giudiziaria.

La segnalazione, effettuata con le modalità di cui all'art. 4 della presente procedura, deve contenere:

- 1) il nominativo e i recapiti del segnalante;
- 2) l'ufficio di appartenenza e la qualifica/mansione svolta;
- 3) la descrizione dei fatti con le circostanze di tempo e di luogo in cui si sono verificati;
- 4) le generalità o altri elementi che consentano di identificare il soggetto cui attribuire il fatto segnalato.

La segnalazione deve inoltre essere corredata degli eventuali documenti che possano suffragare i fatti oggetto di segnalazione, nonché l'indicazione di altri soggetti potenzialmente a conoscenza degli stessi.

Le segnalazioni anonime non rientrano nell'ambito di applicazione della presente procedura.

ART. 4 MODALITÀ DI PRESENTAZIONE DELLE SEGNALAZIONI E SOGGETTI DEPUTATI A RICEVERE E TRATTARE LE SEGNALAZIONI

Canale di segnalazione interna

Il canale di segnalazione interna in Venis, attivato *sentite le organizzazioni sindacali*, è progettato con misure di sicurezza tali da garantire tramite strumenti di crittografia, la riservatezza dell'identità del segnalante, delle persone coinvolte e comunque menzionate nella segnalazione, nonché del contenuto della stessa e della relativa documentazione.

In Venis la gestione del canale interno è affidata al Responsabile della prevenzione della corruzione e della trasparenza, specificamente formato, di cui all'art. 1, c. 7, della L. 6/11/2012, n. 190.

Le segnalazioni in Venis possono assumere forma scritta, anche con modalità informatiche, oppure in forma orale attraverso linee telefoniche o sistemi di messaggistica vocale ma anche, su richiesta del *whistleblower*, mediante un incontro diretto fissato entro un termine ragionevole.

Le modalità, le condizioni e le procedure per effettuare le segnalazioni sono chiare, visibili e facilmente accessibili a tutti i possibili destinatari, anche a chi non frequenta i luoghi di lavoro. Tutte le informazioni sono pubblicate in una sezione dedicata sul sito internet di Venis al fine di assicurarne la conoscenza a tutti i soggetti interessati.

I canali di segnalazione interna assurgono, peraltro, ad oggetto necessario dei modelli di organizzazione e gestione di cui all'articolo 6, comma 1, lett. a) del D.Lgs 231/01.

Treatmento dei dati personali e valutazione d'impatto

In Venis l'intero processo descritto dal D.Lgs. 24/23, e ogni trattamento di dati personali tiene conto e si conforma agli obblighi previsti dal GDPR o del D.Lgs 51/18: l'intera procedura è *compliance* sin dall'inizio, dalla progettazione, alla messa a punto del modello di ricevimento e gestione delle segnalazioni interne, ai rapporti con i fornitori, alle comunicazioni tra i diversi soggetti coinvolti, le informazioni da rendere a tutti i soggetti interessati, i diritti di quest'ultimi, sono stati analizzati i rischi che riguardano tutte le figure coinvolte (*whistleblowers*, persone segnalate, terzi) e adottate le misure tecniche e organizzative idonee a garantire la tutela dei diritti e delle libertà degli interessati e un livello di sicurezza adeguato alla probabilità e alla gravità dei rischi individuati.

Ai sensi dell'art. 13 del Decreto, Venis ha ottemperato all'obbligo di effettuare, prima di avviare il

trattamento già nella fase di progettazione del disegno organizzativo, la Valutazione di impatto sulla protezione dei dati (nel seguito: DPIA) prevista all'art 35 del GDPR, con il coinvolgimento sin dall'avvio del processo del Responsabile della Protezione dei dati di Venis.

In sintesi, Venis al fine di attivare il canale di segnalazione interna, ha:

- disegnato il trattamento allineando, fin dalla progettazione, ogni operazione ai principi di protezione dei dati personali fissati dall'art. 5 del GDPR e dall'art. 3 del D.Lgs.51/18;
- definito i ruoli di responsabilità a partire dalla indicazione del titolare del trattamento (i soggetti tenuti all'obbligo), i designati al trattamento e determinato in modo trasparente, i rispettivi ambiti e responsabilità;
- eseguito la DPIA;
- formato ed autorizzato al trattamento i dipendenti chiamati a gestire il canale di segnalazione;
- redatto e resa disponibile l'informativa privacy nella sezione del sito web dedicata al whistleblowing;
- designato e date istruzioni, in forma scritta, ai "responsabili del trattamento" coloro che sono chiamati ad effettuare il trattamento per conto del titolare, siano essi meri fornitori o gestori del canale. Tali soggetti devono presentare garanzie di compliance alla normativa come prevede l'art. 28 del GDPR;
- previsto che l'esercizio dei diritti di cui agli artt. 15-22 del GDPR sia sottoposto alle limitazioni previste dall'art. 2-undecies del Codice.

Canale di segnalazione esterna

Gli art. 6 e 7 del Decreto regolano condizioni e modalità di esercizio da parte del segnalante, del diritto di attivare una segnalazione esterna. Ciò lascia all'autonoma e discrezionale valutazione del segnalante la decisione di attivare tale percorso al verificarsi di una delle condizioni indicate:

- se nello specifico contesto lavorativo l'attivazione del canale di segnalazione interna non è obbligatoria o il canale non è attivo o non è stato consegnato nel rispetto dei requisiti normativi;
- se il *whistleblower* ha già fatto una segnalazione interna, ma la stessa non ha avuto seguito o si è conclusa con un provvedimento finale negativo;
- se il *whistleblower* ha fondato motivo di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito (ad esempio nel caso in cui sia coinvolto nella violazione il responsabile ultimo del suo contesto lavorativo) ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;
- se il *whistleblower* ha fondato motivo di ritenere che la violazione segnalata possa costituire un pericolo imminente o palese per il pubblico interesse.

L'Anac è il soggetto che ha l'onere di attivare la piattaforma informatica consentendo il corretto funzionamento di tale percorso di segnalazione da parte del *whistleblower* e offrendo le medesime garanzie di riservatezza già indicate per il canale di segnalazione interna.

Le divulgazioni pubbliche

Un'ulteriore modalità di segnalazione (che dovrebbe risultare residuale) è disciplinata dall'art. 15 del D.Lgs. 24/23.

Come per le segnalazioni esterne vengono definite le condizioni al verificarsi delle quali il segnalante può utilizzare tale modalità. Come per la segnalazione esterna la valutazione è lasciata alla discrezionalità del *whistleblower*.

Il soggetto però beneficerà delle medesime misure di protezione accordate dal decreto per l'utilizzo del canale interno/esterno, solo qualora:

- abbia previamente effettuato una segnalazione interna o esterna senza aver ricevuto riscontro nei termini previsti;
- abbia fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- abbia fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di

ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto, come quelle in cui possano essere occultate o distrutte prove oppure in cui vi sia fondato timore che chi ha ricevuto la segnalazione possa essere colluso con l'autore della violazione o coinvolto nella violazione stessa

Permane, infine, la generale clausola di salvaguardia, in favore delle norme sul segreto professionale degli esercenti la professione giornalistica, con riferimento alla fonte della notizia.

ART. 5 GESTIONE DELLE SEGNALAZIONI

La gestione delle segnalazioni in Venis si compone di una valutazione preliminare e di una istruttoria delle stesse.

La trattazione delle segnalazioni, nonché lo svolgimento dell'attività istruttoria della procedura in Venis, sono improntate al rispetto della segretezza dell'identità del segnalante e della riservatezza dei soggetti segnalati.

È definito l'iter procedurale successivo alla segnalazione:

1. entro 7 giorni dalla presentazione, l'incaricato deve rilasciare un avviso di ricevimento al segnalante e ove necessario chiedere integrazioni; mantenere le interlocuzioni e dare diligente seguito;
2. entro 3 mesi occorre fornire riscontro al segnalante 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;
3. entro 7 giorni la segnalazione pervenuta ad un soggetto non competente deve essere inoltrata al corretto destinatario.

Nella valutazione preliminare, il RPCT di Venis effettua un esame sulla sussistenza dei requisiti essenziali che devono essere contenuti nella stessa, al fine dell'attivazione delle tutele di cui all'art. 54-bis del D.Lgs. n. 165/2001. Nel caso in cui dalla valutazione preliminare si rilevi un'evidente e manifesta infondatezza, inammissibilità o irricevibilità, il RPCT procede ad archiviare la segnalazione, dandone notizia al segnalante.

Costituiscono possibili causali di archiviazione:

- a) manifesta mancanza di interesse all'integrità della pubblica amministrazione;
- b) manifesta incompetenza di Venis sulle questioni segnalate;
- c) manifesta infondatezza per l'assenza di elementi di fatto idonei a giustificare gli accertamenti;
- d) manifesta insussistenza dei presupposti di legge per l'avvio dell'istruttoria (condotta illecita ecc.);
- e) accertato contenuto generico della segnalazione tale da non consentire la comprensione dei fatti, ovvero segnalazione corredata da documentazione non appropriata o inconferente;
- f) produzione di sola documentazione in assenza della segnalazione di condotte illecite o irregolarità;
- g) mancanza dei dati indicati nell'art. 3, quali elementi essenziali della segnalazione;
- h) invio reiterato di segnalazioni aventi contenuto uguale o analogo.

Nei casi di cui alle lettere c) e g), non appena ricevuta la segnalazione, il RPCT può chiedere al segnalante di integrare, utilizzando il canale comunicativo della piattaforma informatica dedicata, gli elementi della segnalazione che risultano non adeguatamente circostanziati.

A seguito della positiva valutazione preliminare, il RPCT avvia l'istruttoria interna sui fatti segnalati, che deve terminare entro sessanta giorni lavorativi dalla conclusione della valutazione preliminare.

In ogni momento dell'istruttoria il RPCT può chiedere al segnalante documenti e informazioni ritenute necessarie, sempre utilizzando il canale comunicativo della piattaforma informatica dedicata.

Il RPCT può avanzare richiesta di documentazione o chiarimenti a soggetti interni o esterni all'amministrazione, effettuare audizioni e compiere ogni altro atto istruttorio, nel rispetto della segretezza

dell'identità del segnalante e nel rispetto della riservatezza del segnalato.

Ove ritenuto necessario il RPCT, nel corso dell'esame istruttorio, può avvalersi di soggetti interni all'Amministrazione anche costituendo apposito team di audit, adottando idonee misure a tutela della riservatezza del segnalante e del segnalato.

A tal fine i soggetti del team di audit acquisiscono la qualifica di "soggetti istruttori" della segnalazione.

In casi particolarmente complessi o in caso di necessità di ulteriori approfondimenti istruttori, i termini procedurali indicati possono essere prolungati su richiesta del RPCT fornendo adeguata motivazione.

ART.6 CONCLUSIONE DELL'ISTRUTTORIA

Al termine dell'istruttoria, il RPCT:

a) in presenza di elementi di manifesta infondatezza della segnalazione, ne dispone l'archiviazione con adeguata motivazione, dandone notizia al segnalante;

b) nei casi in cui ravvisi il fumus di fondatezza della segnalazione, provvede alla immediata trasmissione degli atti agli organi preposti interni o istituzioni esterne, ognuno secondo le proprie competenze.

Qualora la segnalazione abbia ad oggetto illeciti che rilevano sotto il profilo penale o erariale, il RPCT provvede alla loro trasmissione alla competente Autorità giudiziaria o contabile, evidenziando che trattasi di una segnalazione pervenuta da un soggetto cui l'ordinamento riconosce la tutela della riservatezza ai sensi dell'art. 54-bis del D.Lgs. n. 165/2001.

Il segnalante è previamente avvisato, con le modalità previste dalla piattaforma informatica dedicata, della eventualità che la sua segnalazione potrà essere inviata all'Autorità giudiziaria e contabile.

ART.7. MISURE DI PROTEZIONE

L'intero Capo III del D.Lgs. 24/23 mira a definire le misure per proteggere i *whistleblowers* sia dalle ritorsioni dirette (quelle rivolte direttamente a loro, come ad esempio il licenziamento, il mobbing, la calunnia...), sia dalle ritorsioni indirette (quelle destinate a colleghi, familiari, i "facilitatori", loro clienti o destinatari dei servizi per i rischi di penalizzazioni o boicottaggio).

Le tutele antidiscriminatorie si applicano in Venis se al momento della segnalazione la persona segnalante aveva fondato motivo di ritenere che le informazioni sulle violazioni segnalate, divulgate pubblicamente o denunciate fossero vere, rientrassero nell'ambito oggettivo ed è stata rispettata la procedura definita dal Decreto. Irrilevanti sono i motivi sottesi alla segnalazione. La *ratio* della norma è quella di incentivare il dipendente a segnalare eventuali comportamenti illeciti, senza che lo stesso abbia timore delle conseguenze pregiudizievoli.

È inoltre prevista, come anche nella disciplina precedente, l'**inversione dell'onere della prova**: la ritorsione si presume posta in essere e l'eventuale danno subito sia conseguenza della segnalazione ed è posto a carico di chi ha compiuto l'atto o il comportamento l'onere di dimostrare che condotte ed atti erano stati era motivati da ragioni estranee alla segnalazione o divulgazione o denuncia.

E il medesimo art. 17 del decreto riporta una ampia indicazione (assolutamente non tassativa) di alcune fattispecie che vengono ricondotte a un comportamento ritorsivo (sanzioni, licenziamento, demansionamento, trasferimento, misure discriminatorie, dirette o indirette, comprensive anche dei danni reputazionali, "in particolare sui social media").

L'articolo 18 disciplina le misure di sostegno a favore della persona segnalante e legittima l'autorità giudiziaria o amministrativa cui la persona segnalante si sia rivolta per ottenere protezione dalle ritorsioni, a richiedere all'Anac informazioni e documenti relativi alla segnalazione.

Rimane in capo ad Anac la competenza a ricevere le segnalazioni di possibili ritorsioni, ad avviare l'attività istruttoria, a segnalare le fattispecie di competenza agli organismi e ad applicare le sanzioni previste.

Tra le ulteriori misure di protezione vanno collocate:

- la nullità di eventuali rinunce e transazioni relative a diritti e alle tutele previste dal decreto;
- un'esimente generale (che esclude anche la responsabilità civile e amministrativa, oltre a quella

penale) in favore del soggetto che effettui (ai sensi dell'art.16) la segnalazione, denuncia o divulgazione pubblica di informazioni coperte da segreto, da prerogative autoriali o tutelate dalla disciplina di protezione dati, purché al momento della rivelazione sussistessero fondati motivi per ritenerla necessaria per svelare la violazione;

- viene esclusa ogni altra responsabilità per l'acquisizione o l'accesso alle informazioni sulle violazioni, salva l'ipotesi in cui la condotta costituisca reato. Esimente però esclusa per le condotte non strettamente necessarie a rivelare la violazione o, comunque, non collegate alla segnalazione, denuncia o divulgazione pubblica.

Nel dettaglio in Venis è previsto che:

- l'identità del segnalante non può essere rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni;
- la protezione riguarda non solo il nominativo del segnalante ma anche tutti gli elementi della segnalazione dai quali si possa ricavare, anche indirettamente, l'identificazione del segnalante;
- la segnalazione è sottratta all'accesso agli atti amministrativi e al diritto di accesso civico generalizzato;
- la protezione della riservatezza è estesa all'identità delle persone coinvolte e delle persone menzionate nella segnalazione fino alla conclusione dei procedimenti avviati in ragione della segnalazione, nel rispetto delle medesime garanzie previste in favore della persona segnalante

ART. 8. PROCEDURA TRASMISSIONE/ RICEZIONE /GESTIONE SEGNALAZIONI

Le segnalazioni sono gestite tramite un sistema applicativo informatico che garantisce strumenti di crittografia sui contenuti testuali e sui file allegati e che non ha alcuna possibilità di accesso alle segnalazioni. Il segnalante, effettuata la registrazione alla piattaforma informatica dedicata, raggiungibile tramite link presente sul sito istituzionale, è abilitato a formulare la segnalazione, inserendo i dati ed eventuali allegati, e ad inviarla al RPCT.

E' previsto inoltre che le segnalazioni avvengano in forma orale attraverso una linea telefonica dedicata con messaggistica vocale ove sarà registrata la segnalazione. E' previsto inoltre, su richiesta del *whistleblower*, un incontro diretto fissato entro un termine ragionevole.

Il sistema informatico provvede alla cifratura e alla memorizzazione della segnalazione, separandola dall'identità del segnalante e inviando una e-mail di notifica al RPCT e una di notifica di avvenuto invio al segnalante stesso.

La segnalazione viene presa in carico dal RPCT che, nella sua area riservata, può gestirne l'istruttoria.

Il segnalante, accedendo alla propria area riservata, ha la possibilità di seguire l'iter della propria segnalazione.

Le segnalazioni e la relativa documentazione allegata sono sottratte al diritto di accesso agli atti amministrativi di cui all'art. 22 e ss. della L. n. 241/1990 nonché all'accesso civico generalizzato di cui all'art. 5, comma 2, del D.Lgs. n. 33/2013.

FASE 1 – ACCESSO E COMPILAZIONE

Il segnalante accede al sito internet aziendale www.venis.it all'interno del quale è sviluppato l'applicativo di gestione delle segnalazioni e compila la segnalazione.

FASE 2 – COMUNICAZIONE DELLE CREDENZIALI DI CONSULTAZIONE

Successivamente all'inoltro della segnalazione, il segnalante riceve dal sistema un codice identificativo univoco (all'indirizzo mail indicato in fase di compilazione della segnalazione) e una password (all'interno della pagina web a chiusura dell'iter di segnalazione) per la consultazione da utilizzare per successivi accessi.

FASE 3 – INOLTRO AL RESPONSABILE DELLA PREVENZIONE DELLA CORRUZIONE

I dati della segnalazione (unitamente ai vari documenti allegati) e scorporati dai dati identificativi del segnalante, vengono automaticamente inoltrati, per l'avvio tempestivo dell'istruttoria, al Responsabile

della prevenzione della corruzione; il Responsabile riceverà una comunicazione via e-mail di avvenuta presentazione di una segnalazione, con il codice identificativo della stessa (senza ulteriori elementi di dettaglio). Il Responsabile ha a disposizione delle proprie credenziali di accesso al sito all'interno del quale è sviluppato l'applicativo, grazie ad esse può accedere ad una pagina di sintesi e da questa accedere alle informazioni di dettaglio delle varie segnalazioni ricevute. I dati identificativi del segnalante sono custoditi, in forma crittografata, e sono accessibili ai sensi della normativa solamente al Responsabile della Sicurezza Informatica individuato da Venis S.p.A. ai sensi di legge.

FASE 4 – ITER DELLA SEGNALAZIONE

Il Responsabile della prevenzione della corruzione, che eventualmente può avvalersi di un gruppo di lavoro ad hoc, prende in carico la segnalazione per una prima sommaria istruttoria. Se indispensabile, richiede chiarimenti al segnalante e/o a eventuali altri soggetti coinvolti nella segnalazione con l'adozione delle necessarie cautele, provvedendo alla definizione dell'istruttoria nei termini di legge.

I dati e i documenti oggetto delle segnalazioni vengono trattati a norma di legge e l'accesso agli atti, da parte dei soggetti autorizzati, è opportunamente regolamentato dalle politiche di sicurezza informatica di Venis S.p.A..

Si precisa che resta impregiudicato il diritto del lavoratore a ricorrere all' Autorità Giudiziaria competente.

FASE 5 – CONSULTAZIONE DA PARTE DEL SEGNALANTE

Il segnalante può monitorare lo stato di avanzamento dell'istruttoria accedendo al sistema di gestione ed utilizzando il codice identificativo e la password ricevuti in fase di compilazione.

FASE 6 – PUBBLICAZIONE DATI DI SINTESI

Il Responsabile della prevenzione della corruzione si riserva di pubblicare, nella pagine "Amministrazione Trasparente" del sito istituzionale una sintesi del numero di segnalazioni ricevute e del loro stato di avanzamento, con modalità tali da garantire comunque la riservatezza dell'identità dei segnalanti.

ART. 9. ATTIVITA' DEL RESPONSABILE DELLA PREVENZIONE DELLA CORRUZIONE

Il Responsabile della prevenzione della corruzione, in accordo alle previsioni ANAC, invia a tutto il personale della Società, con cadenza periodica, comunicazioni ed informative specifiche in cui sono illustrate le finalità dell'istituto del "whistleblowing".

Il Responsabile della prevenzione della corruzione rende conto nella Relazione Annuale di cui all'art. 1 comma 14 della Legge 190/2012, con modalità tali da garantire la riservatezza dei segnalanti, del numero di segnalazioni ricevute e del loro stato di avanzamento.

Il Responsabile della prevenzione della corruzione provvederà a pubblicare il presente regolamento sia sulla intranet aziendale sia sul sito internet aziendale www.venis.it nella sezione SOCIETA' TRASPARENTE/ ALTRI CONTENUTI/PREVENZIONE DELLA CORRUZIONE/ WHISTLEBLOWING.

Il Responsabile della prevenzione e della corruzione può essere supportato dall'eventuale suo Vice che custodisce copia della chiave.

La trattazione delle segnalazioni, nonché lo svolgimento dell'attività istruttoria della presente procedura, sono improntate al rispetto della segretezza dell'identità del segnalante e della riservatezza dei soggetti segnalati.

Qualora le segnalazioni riguardino una condotta tenuta dal RPCT, le stesse dovranno essere inviate direttamente all'ANAC, avvalendosi delle procedure dedicate. Il segnalante ha la facoltà di rendere nota la propria identità al RPCT.

Le Linee Guida 469/2021 stabiliscono inoltre che il custode delle identità laddove individuato può consentire al RPCT, su richiesta, di accedere all'identità del segnalante, in presenza di comprovate e idonee motivazioni che hanno reso necessaria la conoscenza dell'identità del segnalante.

Venis ha previsto la possibilità dell'eventuale nomina del custode e si rifà alle norme di legge quanto ai casi e alle motivazioni in presenza delle quali il custode delle identità può consentire l'accesso all'identità

del segnalante.

Laddove in Venis le figure del custode e del RPCT coincidessero, questi potrà accedere all'identità del segnalante in presenza di idonee motivazioni sempre nel rispetto della legge. Venis registrerà tale accesso, dando conto delle motivazioni specifiche che hanno reso necessaria la conoscenza dell'identità del segnalante.

L'identità del segnalante non è nota al custode. Non è coinvolto nel trattamento dati personali presenti nella segnalazione”.

ART. 10 PRIVACY E RISERVATEZZA

Venis nel rispetto della disciplina in tema di protezione dei dati personali si è prefissata l'esigenza di perseguire il principio di minimizzazione dei dati trattati. A tal fine rispetta la tutela dell'identità della persona segnalante e della riservatezza quale strumento per incoraggiare il soggetto che viene a conoscenza di illeciti a trasmettere la relativa segnalazione.

Venis ha redatto e resa disponibile l'informativa privacy nella sezione del sito web dedicata al whistleblowing.

In particolare:

- l'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, non potrà essere rivelate, senza il consenso espresso della stessa persona segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati;
- ogni segnalazione resa oralmente (in colloqui oppure mediante linee telefoniche registrata) viene riportata nella piattaforma utilizzata da Venis;
- la segnalazione e la documentazione allegata è sottratta al diritto di accesso ai documenti amministrati;
- le segnalazioni non possano essere utilizzate per scopi diversi, né rivelate a persone diverse da quelle specificamente competenti, autorizzate ed istruite in assenza del suo consenso espresso;
- nell'ambito del procedimento penale, l'identità del segnalante è coperta da segreto ai sensi dell'articolo 329 c.p.p.; nel procedimento dinanzi alla magistratura contabile essa non può essere rivelata sino alla chiusura della fase istruttoria; nell'ambito del procedimento disciplinare, invece, l'identità del segnalante non può essere rivelata ove la contestazione dell'illecito disciplinare si fonda su accertamenti distinti e ulteriori rispetto alla segnalazione mentre occorre il consenso se la stessa sia indispensabile per la difesa dell'incolpato;
- l'identità delle persone coinvolte e di quelle menzionate nella segnalazione è garantita sino alla conclusione dei relativi procedimenti, con il rispetto delle stesse garanzie accordate al segnalante;
- la conservazione delle segnalazioni interne ed esterne e della relativa documentazione è consentita per il tempo necessario alla loro definizione e, comunque, per oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione.

ART. 11 SANZIONI

Il Decreto rafforza il potere di intervento dell'Anac ampliandone i settori di competenza, le modalità di intervento e fissando le sanzioni amministrative pecuniarie applicabili in caso di accertamento di violazioni nei confronti di tutti i soggetti obbligati dalla nuova disciplina.

Le sanzioni devono essere effettive, proporzionate e dissuasive.

Fermo restando altri profili di responsabilità l'Anac applica:

da € 10.000 a € 50.000 quando accerta che:

- sono state commesse ritorsioni;
- la segnalazione è stata ostacolata o che si è tentato di ostacolarla o è stato violato l'obbligo di riservatezza;
- non sono stati istituiti canali di segnalazione o non sono state adottate procedure per l'effettuazione e la gestione delle segnalazioni ovvero l'adozione o la loro implementazione non è

- conforme alla normativa;
- non è che non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute.

da € 500 a € 2.500 quando accerta che è stato violato l'obbligo di riservatezza circa l'identità del segnalante.

Venis al fine di rafforzare le misure a tutela della riservatezza del segnalante, prevede nel proprio codice di comportamento e disciplinare responsabilità specifica e sanzioni in capo sia al RPCT che riceve e gestisce le segnalazioni di whistleblowing, sia a tutti gli altri soggetti - ivi inclusi i componenti del gruppo di lavoro- che in Venis possano venire a conoscenza delle segnalazioni, con i dati e le informazioni in essa contenuti per i quali si accertano responsabilità di illeciti.

ART. 12. AVVICENDAMENTO DEL RPCT

In caso di avvicendamento del RPCT relativamente alle segnalazioni già ricevute, Venis prevede, secondo i principi di ragionevolezza e continuità dell'azione amministrativa, che necessariamente il nuovo RPCT abbia accesso alle segnalazioni ricevute anche dal RPCT precedente, soprattutto ove il procedimento sulla segnalazione non si sia ancora concluso.

Il ruolo fondamentale nella gestione delle segnalazioni è infatti attribuito direttamente dalla legge al soggetto cui l'amministrazione conferisce l'incarico di RPCT.

Nel caso in cui il RPCT si avvallesse di un team o di un ufficio apposito, i componenti del team sono autorizzati ad accedere alle informazioni e ai dati contenuti nella segnalazione.

In Venis tali soggetti sono precedentemente individuati e nominati, definendo le responsabilità in tutte le fasi del processo di gestione delle segnalazioni, con particolare riguardo agli aspetti di sicurezza e di trattamento delle informazioni.

Nell'ambito dell'ufficio competente in materia di whistleblowing, spetta al RPCT l'assegnazione della competenza sulle singole segnalazioni ai componenti del team. L'assegnazione può anche essere revocata con provvedimento motivato.