ALLEGATO "E" al PTPC 2021-2023
WHISTLEBLOWER

POLICY SULL'UTILIZZO E LA GESTIONE DEL
SISTEMA DI SEGNALAZIONE DI CONTOTTE ILLECITE

PREMESSA.

La Legge n. 190/2012 (*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione*) ha introdotto, per la prima volta nell'ordinamento nazionale, all'art. 1, comma 51, una norma a tutela del dipendente (pubblico e privato) che segnala condotte illecite dall'interno dell'ambiente di lavoro (c.d. *"whistleblower"*). «*Fuori dei casi di responsabilità a titolo di calunnia o diffamazione, il pubblico dipendente che denuncia all'autorità giudiziaria o alla Corte dei conti, ovvero riferisce al proprio superiore gerarchico condotte illecite di cui sia venuto a conoscenza in ragione del rapporto di lavoro, non può essere sanzionato, licenziato o sottoposto ad una misura discriminatoria, diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla denuncia*».

Liguria Digitale, a recepimento di tale norma e sulla base della determinazione ANAC n. 6/2015 "*Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. whistleblower)*", ha adottato un "***Sistema interno di segnalazione delle violazioni***" (o "*Sistema di whistleblowing"*) a disposizione di chiunque ritenga di segnalare condotte illecite che possano arrecare danno o pregiudizio alla Società. La finalità specifica di tale Sistema è quella di far emergere, individuare e combattere eventuali fenomeni corruttivi o comunque illeciti, per tutelare l'azionariato da danni economici e all'immagine, per diffondere la cultura dell'etica, della legalità e della trasparenza all'interno della Società.

Il "*Sistema di whistleblowing"*, informatizzato dalla Società nel 2016, recepisce oggi anche le modifiche normative introdotte dalla Legge n. 179/2017 *"Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato*" e le "*Indicazioni*" fornite dall'ANAC il 05/09/2018 "*per la migliore gestione delle segnalazioni di illeciti o irregolarità*".

La **presente Policy** regolamenta, quindi, il *Sistema di whistleblowing* e l'utilizzo dello strumento informatico precisando, sulla base delle modifiche normative intervenute e delle linee guida ANAC:

1. i soggetti del processo di whistleblowing;
2. il perimetro delle condotte, avvenimenti o azioni che possono essere oggetto di segnalazione;
3. i principi e le regole generali a tutela del segnalante;
4. il sistema web di *whistleblowing* e il procedimento di valutazione delle segnalazioni;
5. le segnalazioni pervenute al di fuori del Sistema web.

1. I SOGGETTI DEL PROCESSO DI WHISTLEBLOWING

1.1 Il *segnalante* o *"whistleblower"*.

Il "*segnalante*" o *"whistleblower"* è la persona fisica, interna o esterna a Liguria Digitale, che segnala eventuali illeciti a cui abbia assistito o di cui sia venuto a conoscenza in ragione dello svolgimento della propria attività lavorativa con la Società o in occasione e/o a causa dello svolgimento delle mansioni lavorative assegnategli dalla stessa.

1.2 Il *Segnalato*.

Il "*segnalato*" è il membro degli organi societari, il dirigente, il dipendente, il collaboratore esterno, il fornitore, il cliente o il partner di Liguria Digitale al quale sia riferibile la condotta illecita di cui il *"whistleblower"* sia venuto a conoscenza.

1.3 Il *Comitato di whistleblowing.*

Il *Comitato di whistleblowing* è l'organismo aziendale responsabile del procedimento e, quindi, della presa in carico e verifica di ogni segnalazione di condotta illecita ricevuta dalla Società e della tutela del dipendente che le effettua come indicato al successivo § 3.
In osservanza alla Legge n. 190/2012 e al D.lgs. n. 231/2001:

è costituito da	▪ il RPCT (Responsabile della Prevenzione della Corruzione e della Trasparenza) ▪ l'ODV (Organismo di Vigilanza) 231;
si avvale	▪ della Struttura di Supporto operativo del RPCT; ▪ della Funzione Internal Audit;
opera	▪ con indipendenza e imparzialità. Nel caso in cui emergano, all'atto della presa in carico della segnalazione e in ogni fase successiva del procedimento, situazioni di potenziale conflitto di interessi, il componente/i che si trovi in tale situazione si astiene e il Comitato procede carente di tale componente. In tale ipotesi verrà ad esso/i precluso l'accesso al procedimento e ad ogni informazione attinenti a tale segnalazione.

2. IL PERIMETRO DELLE CONDOTTE, AVVENIMENTI O AZIONI CHE POSSONO ESSERE OGGETTO DI SEGNALAZIONE.

2.1 Oggetto delle segnalazioni

A norma dell'art. 1, comma 1, della Legge n. 179/2017, le segnalazioni che hanno rilevanza nel *Sistema di Whistleblowing* sono esclusivamente quelle che hanno ad oggetto **condotte illecite** di personale dirigente/dipendente, di collaboratori e/o di clienti/fornitori di Liguria Digitale **di cui il Segnalante sia venuto direttamente a conoscenza in ragione del proprio rapporto di lavoro**

Trattasi, quindi, di segnalazioni afferenti a condotte illecite

che costituiscono:	1. reati a norma della Legge n. 190/2012 (c.d. Legge anticorruzione) 2. reati a norma del D.Lgs. n. 231/2001; 3. abuso di potere per ottenere vantaggi privati; 4. violazioni del Codice Etico o di altre disposizioni aziendali sanzionabili in via disciplinare;
che riguardino:	situazioni di cui il soggetto sia venuto direttamente a conoscenza «in ragione del rapporto di lavoro» e, quindi, ricomprendono certamente quanto si è appreso in virtù dell'ufficio rivestito ma anche quelle notizie che siano state acquisite in occasione e/o a causa dello svolgimento delle mansioni lavorative, seppure in modo casuale.

Nel *Sistema di Whistleblowing* non rilevano, invece, le segnalazioni relative a questioni di natura personale o a istanze che rientrano nella disciplina del rapporto di lavoro e/o nei rapporti con il superiore gerarchico o i colleghi che continuano a dover essere gestite con le ordinarie prassi aziendali e con gli uffici competenti.

Tale sistema, precisa l'ANAC:

- *"NON tutela diritti e interessi individuali";*
- *"NON svolge attività di accertamento/soluzione di vicende soggettive e personali del segnalante";*
- *"NON può sostituirsi alle istituzioni competenti per materia";*
- *"NON fornisce rappresentanza legale o consulenza al segnalante".*

2.2 Elementi essenziali della segnalazione

Le segnalazioni, ai fini della loro validità, devono essere qualificate dai seguenti elementi "*essenziali*":

- l'identità del segnalante (nel rispetto della garanzia di riservatezza di cui al seguente § 3);
- la qualificazione della condotta illecita oggetto di segnalazione (che deve essere riconducibile a reati penali, abuso di potere per ottenere vantaggi privati o violazioni del Codice Etico o di altre disposizioni aziendali sanzionabili in via disciplinare);
- la descrizione circostanziata del fatto atta a permetterne la comprensione, il periodo temporale in cui si è verificato ed ogni ulteriore informazione e/o documentazione che possano confermare la fondatezza del fatto segnalato.
  Considerato lo spirito della norma - che è quello di incentivare la collaborazione di chi lavora all'interno della Società per l'emersione dei fenomeni corruttivi - non è richiesta, ai fini dell'ammissibilità della segnalazione, l'assoluta certezza dell'effettivo avvenimento dei fatti denunciati e dell'autore degli stessi, essendo invece sufficiente che il Segnalante, in base alle proprie conoscenze, ritenga altamente probabile che si sia verificato un fatto illecito nel senso sopra indicato. In questa prospettiva è opportuno che le segnalazioni siano il più possibile circostanziate e offrano il maggior numero di elementi al fine di consentire alla Società di effettuare le dovute verifiche.
  Non sono invece ammissibili le segnalazioni fondate su meri sospetti o voci.

3. I PRINCIPI E LE REGOLE GENERALI A TUTELA DEL SEGNALANTE.

3.1 Distinzione tra segnalazione anonima e riservatezza dell'identità del segnalante

Liguria Digitale, in ottemperanza al disposto normativo, assicura la riservatezza dell'identità del Segnalante sin dalla ricezione della segnalazione e in ogni fase successiva.

La garanzia di riservatezza presuppone, come precisato dall'ANAC, "*che il segnalante renda nota la propria identità. Non rientra, dunque, nella fattispecie prevista dalla norma come «dipendente che segnala illeciti», quella del soggetto che, nell'inoltrare una segnalazione, non si renda conoscibile. In sostanza, la ratio della norma è di assicurare la tutela del dipendente, mantenendo riservata la sua identità, solo nel caso di segnalazioni provenienti da dipendenti individuabili e riconoscibili*".

3.2 Tutela del segnalante.

La tutela del dipendente che segnala reati o condotte illecite è garantita da Liguria Digitale, in piena osservanza alla normativa vigente, attraverso:

a) il divieto di discriminazione. Il segnalante non può essere sanzionato, licenziato o sottoposto ad alcuna misura discriminatoria, diretta o indiretta, avente effetti sulle condizioni di lavoro per motivi collegati direttamente o indirettamente alla denuncia. Alla violazione di tale divieto sono comminate, per legge, sanzioni amministrative a carico del responsabile che, peraltro, ne risponde anche a titolo di responsabilità disciplinare;

b) la garanzia di riservatezza. L'identità del segnalante, seppur sia elemento essenziale per l'ammissibilità della segnalazione, resta riservata sin dalla ricezione della segnalazione e in ogni fase successiva e può essere rivelata solo nei casi tassativamente normati dall'articolo 1, comma 3, della Legge n. 179/2017 e, quindi:
   - nel procedimento penale o in quello amministrativo davanti alla Corte dei Conti: a conclusione della fase istruttoria, qualora il mantenimento dell'anonimato pregiudichi la possibilità dell'accusato, rinviato a giudizio, di difendersi;

- nel procedimento disciplinare ove ricorrano contestualmente le seguenti 3 condizioni:
  - la contestazione sia fondata esclusivamente sulla segnalazione;
  - la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato;
  - il segnalante abbia fornito, in sede di trasmissione della segnalazione stessa, il consenso alla rivelazione della sua identità;

c) l'esclusione dall'accesso agli atti. In ogni caso la segnalazione e l'identità del segnalante sono esclusi dall'accesso ai documenti amministrativi previsto dalla Legge n. 241/1990 e dal D.lgs n. 33/2013.

Resta inteso che l'impianto normativo a tutela del segnalante non è garantito, a norma dell'art. 1, comma 9, della Legge n. 179/2017, "*nei casi in cui sia accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante*" stesso "*per i reati di calunnia e diffamazione*".
La violazione del divieto di discriminazione o del sistema a tutela della riservatezza del Segnalante è fonte di responsabilità disciplinare, salve le ulteriori forme di responsabilità e di sanzioni prescritte dalla Legge n. 190/2012.

IL SISTEMA WEB DI WHISTLEBLOWING E IL PROCEDIMENTO DI VALUTAZIONE DELLE SEGNALAZIONI.

3.3 Sistema web di whistleblowing

Liguria Digitale, al fine di favorire segnalazioni di eventuali condotte illecite e di proteggere la riservatezza dell'identità del segnalante, mette a disposizione del proprio personale dipendente e dei terzi un **Sistema web**:

- accessibile con qualsiasi dispositivo al link https://liguriadigitale.azurewebsites.net oltre che dalla intranet aziendale;
- basato su protocollo di crittografia che garantisce una rafforzata tutela della riservatezza dell'identità del segnalante che resta anonima in ogni fase del processo e che permette allo stesso di dialogare in modo spersonalizzato e rapido con la Società.

3.4 Presentazione della segnalazione.

Il segnalante accede al Sistema web di *whistleblowing* e registra, attraverso lo stesso, la segnalazione. In questa fase, il segnalante è tenuto a:

- identificarsi. E' il Sistema, infatti, ricevuta la segnalazione a criptare in modo automatico i dati del segnalante inserendoli in un archivio informatico separato e protetto e ad attribuire alla segnalazione stessa un codice identificativo univoco;
- assegnare una categoria alla propria Segnalazione che deve essere riconducibile a:
  1. reati a norma della Legge n. 190/2012 (c.d. Legge anticorruzione)
  2. reati a norma del D.Lgs. n. 231/2001;
  3. abuso di potere per ottenere vantaggi privati;
  4. violazioni del Codice Etico o di altre disposizioni aziendali sanzionabili in via disciplinare;
- inserire gli ulteriori elementi essenziali della segnalazione di cui al precedente § 2.2.

3.5 Presa in carico e verifica preliminare della segnalazione

La segnalazione, una volta ricevuta dal Sistema web e previa criptazione dei dati del segnalante, è presa in carico dal *Comitato di whistleblowing* che procede a una prima verifica del contenuto dei fatti riferiti, da concludersi nel più breve tempo possibile e in ogni caso non oltre quindici giorni.

Qualora la segnalazione risulti:

a. manifestatamente infondata o i fatti non rientrino tra le condotte illecite a norma dell'art. 1, comma 1, della Legge n. 179/2017, il Comitato procede alla sua archiviazione;
b. non manifestatamente infondata e i fatti rientrino tra le condotte illecite a norma dell'art. 1, comma 1, della Legge n. 179/2017, il Comitato avvia l'istruttoria.

3.6 Istruttoria

Ai fini dell'istruttoria, il *Comitato di whistleblowing* può avvalersi della Struttura di supporto operativo del RPCT (istituita a norma dell'art. 1, comma 8, della Legge n. 190/2012) e della Funzione di Internal Audit che svolgono, congiuntamente o in modo autonomo, le verifiche ritenute necessarie od opportune sulla base dei seguenti elementi:

- informazioni fornite a corredo della segnalazione o trasmesse dal Segnalante anche in un secondo momento, a richiesta del Comitato o spontaneamente a integrazione dei fatti riferiti. Proprio al fine di permettere lo svolgimento di un'effettiva istruttoria, è richiesto al Segnalante stesso di accedere periodicamente al Sistema verificando, attraverso il codice univoco attribuitogli all'atto della registrazione della segnalazione, se vi siano richieste di chiarimenti e/o di ulteriori informazioni sui fatti segnalati;
- attuali procedure in vigore attinenti i fatti segnalati;
- segnalazioni/verifiche precedenti aventi lo stesso oggetto e già esaminate;
- eventuali indagini già in corso da parte di pubbliche autorità sui fatti oggetto di segnalazione.

Qualora in esito a tali verifiche istruttorie il *Comitato di whistleblowing*:

- ritenga di disporre di tutti gli elementi necessari e utili alla verifica della segnalazione, procede a chiudere l'istruttoria e alla valutazione conclusiva di cui al successivo § 4.5;
- ravvisi la necessità di ulteriori verifiche, presso le strutture aziendali interessate o le persone coinvolte, trasmette alle stesse la segnalazione in formato completamente anonimo. Tali strutture aziendali interessate o persone coinvolte dovranno formulare le proprie valutazioni entro e non oltre quindici giorni dalla ricezione della richiesta.

L'istruttoria è completata entro 30 giorni dalla conclusione della fase di cui al § 4.3 - fatti salvi i casi in cui segnalazioni relative a situazioni di particolare complessità richiedano tempi di istruttoria più lunghi e comunque non superiori a 60 giorni - nel rispetto dei principi di imparzialità, competenza e diligenza professionale.

3.7 Valutazione conclusiva.

All'esito dell'istruttoria il Comitato di whistleblowing provvede a predisporre una valutazione conclusiva o a far propria quella della Struttura a Supporto del RPCT e/o della funzione Internal Audit di cui si sia avvalso, e a indicare le eventuali azioni correttive e/o disciplinari ritenute necessarie.

Resta inteso che qualora in relazione alla natura della violazione sussistano le condizioni di legge, il Comitato e/o i singoli organi che lo compongono, congiuntamente o singolarmente, presentano denuncia all'Autorità Giudiziaria competente.

La chiusura delle verifiche è registrata attraverso il Sistema Web e, quindi, comunicata al Segnalante.

Salvo il caso in cui la segnalazione abbia ad oggetto comportamenti ascrivibili all'Amministratore Unico e/o ad uno o più componenti del Collegio Sindacale, il Comitato di whistleblowing provvede a fornire ai suddetti organi, trimestralmente o con immediatezza in caso di denuncia, informativa in merito alle segnalazioni e all'esito della loro valutazione.

3.8 Informativa al segnalato

Nell'ambito di tutte le fasi di gestione delle segnalazioni il Comitato valuta l'opportunità di procedere ad informare il soggetto segnalato in merito all'effettuazione di una segnalazione a suo carico, allo svolgimento del procedimento e all'esito dello stesso. In particolare, il momento in cui il segnalato verrà messo al corrente della segnalazione a suo carico sarà valutato caso per caso, verificando se tale informativa possa, o meno, inficiare le necessarie indagini per l'accertamento della segnalazione o se, invece, il coinvolgimento del segnalato sia necessario per l'indagine stessa.

4. LE SEGNALAZIONI PERVENUTE AL DI FUORI DEL SISTEMA WEB.

Il Sistema di Segnalazione Web è per Liguria Digitale il canale preferenziale di whistleblowing. Tale Sistema, infatti, garantisce la tutela della riservatezza del Segnalante, la tracciabilità di ogni fase del processo e la certezza dei tempi.

Resta inteso che verranno tenute in considerazione anche quelle segnalazioni pervenute al di fuori di tale Sistema, attraverso l'utilizzo degli indirizzi e-mail anticorruzione@liguriadigitale.it o odv231@liguriadigitale.it, ove siano qualificate dagli elementi essenziali di cui al precedente § 2.2. In tali casi, il RPCT e l'ODV231 si danno reciproca comunicazione delle segnalazioni singolarmente ricevute.